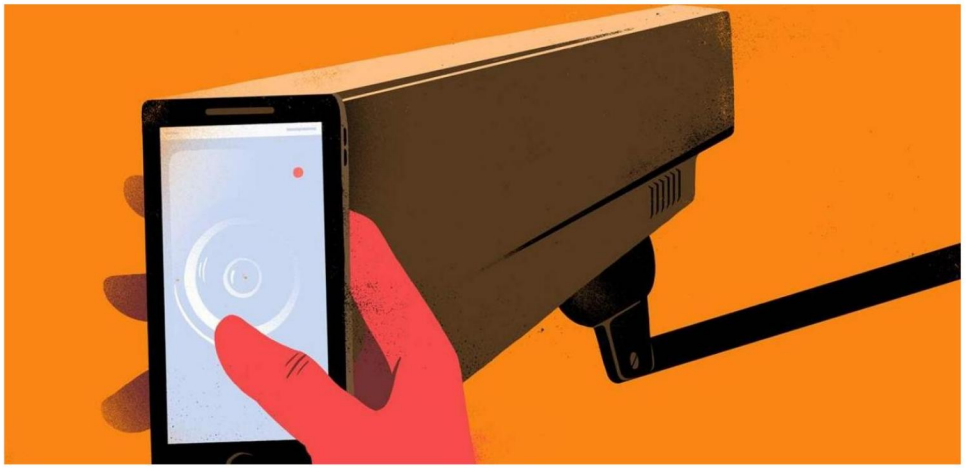
Cette brochure veut recenser des problématiques liées à la surveillance policière des téléphones, et donner des petites astuces pour réduire les risques liés à celle-ci.

Il s'agit ici de la troisième version de cette brochure. Elle comporte des erreurs, raccourcis, incertitudes. De plus, tout ce qui a trait au numérique évolue vite. N'hésite pas à en faire des critiques pour faire évoluer ce texte, via le contact :

autodefense-numerique@riseup.net

Téléphonie mobile

Surveillances, répressions, réduction des risques



3ème version : Septembre 2025

Table des matières

Ressources supplémentaires

• Site internet de La Quadrature du Net sur l'évolution des lois numériques : https://laquadrature.net
• No Trace Project (https://notrace.how)
• Surveillance Self-Défense (anglais/français), avec plusieurs guides pratiques sur téléphone: https://ssd.eff.org/fr/module-categories/guides-sur-les-outils
• Guide sur la sécurité des téléphones portables et sécurité des activistes (en anglais). "Mobile Phone Security for Activists and Agitators"
• Guide d'autodéfense numérique pour tout ce qui touche aux ordinateurs : https://guide.boum.org
• Vidéos de Christophe Boutry sur sa chaîne youtube @Ced_haurus (explications et tutos sur la téléphonie mobile)
• Listes logiciels libres alternatifs (logiciel libre ne veut pas dire sécurisé pour ce que tu veux faire) :
- https://technopolice.be/autodefense-numerique/
- https://www.chatons.org/
- ***https://riseup.net/fr/security/resources/radical-servers***

Lexique

Logiciel libre vs logiciel propriétaire
Avant de continuer il est important de comprendre la différence.
Un **logiciel libre** ou **open source**, sont des logiciels dont on a accès au code source, c'est-à-dire dont on peut avoir accès à la recette du logiciel pour savoir comment il fonctionne (le logiciel libre va plus loin car il offre la liberté de modifier, redistribuer, modifier le logiciel en plus d'avoir accès à la recette).
Le **logiciel propriétaire** n'offre pas l'accès au code source. Cela signifie qu'il ne peut pas y avoir d'avis extérieur à la structure qui fourni le logiciel propriétaire, on remet 100 % de notre confiance à l'entreprise qui a créé le logiciel en terme de sécurité et de respect de nos données personnelles.

Information en claire vs information chiffrée
Une information est dite en « **claire** » si toute personne / machine qui y a accès peut avoir accès au contenu directement.
Une information est dite chiffrée quand elle nécessite l'utilisation d'une clé de déchiffrement pour accéder au contenu. Le chiffrement (ou
le déchiffrement) d'une information se fait grâce à un algorithme de chiffrement. Il en existe de différents types, de qualités et aux fonctionnalités variables.

Client : en informatique, un logiciel client se connecte à un serveur pour accéder à des services ou des données (mails, messageries, navigateurs, etc.)
Fork : C'est un nouveau logiciel créé à partir du code source d'un logiciel existant. Son existence découle d'un choix politique venant de visions différentes du projet des différents acteurs qui y participent, un acteur décidant alors de créer cette *dérivation* pour lui imposer les idées qu'il n'a pas pu soumettre au précédent projet,
Métadonnées : Les métadonnées, c'est ce qui décrit le contexte autour de la donnée. Dans un SMS il y a la donnée qui est le SMS en tant que telle, la métadonnée c'est la taille du SMS, qui écrit à qui, à quelle heure, etc.

Introduction

Ce texte a été effectué car on manque de ressources sur cette thématique dans les milieux militants. Certaines parties parlent des problématiques de surveillance policière liée à la téléphonie de manière générale, elles sont symbolisées en début de chapitre par [ ] et dans la table des matières par []. Ces parties traitent les problématiques à la fois pour les téléphones à bouton et pour les smartphones. D'autres parties parlent plus des smartphones ( ). Les mots avec une * sont explicités dans un lexique à la fin de la brochure.

On trouve plus d'outils de réduction des risques pour les smartphones, mais on retrouve les mêmes problématiques qu'avec les téléphones à boutons, et les smartphones ont aussi d'autres problématiques en termes de sécurité. Parfois les outils offrent des sensations de sécurité qui font oublier leurs limites, et poussent à diffuser des informations sensibles qu'on aurait mieux fait de faire passer par d'autres canaux.

Si l'angle de ce document se porte sur les enjeux de surveillance et les outils de sécurité vis-à-vis de la répression de l'État, on pourrait aborder ces problématiques par d'autres angles, que ce soit en usage collectif ou individuel :

- Écologie et colonialisme car il faut 70 matériaux différents et 70 kg de matière extraite et assemblée par des personnes sous-payées, dans des pays colonisés par le capitalisme pour construire un smartphone qui sera détruit rapidement[1]

- Résistance à la pression de passer toujours plus par ces outils, pour le travail ou les administrations, la banque, les démarches de santé et autres et qu'il y a souvent plein d'astuces à se transmettre pour ne pas avoir à fournir de numéro de téléphone ou pour pouvoir rester déconnecté·e

- Que ces outils sont aussi des sources d'exclusion pour les personnes qui n'y ont ou ne souhaitent pas y avoir accès, ou qui manquent de compétences. Il est important au sein des collectifs d'avoir des discussions à ces sujets pour que la sécurité ne devienne pas un outil de domination pour certain·es.

- Défense de nos données contre les multinationales, même si certaines propositions se recoupent car les multinationales sont très régulièrement sollicitées par les flics[2].

1 Voir pour l'analyse le dossier par exemple de « L'empreinte cachée des smartphones » de France Nature Environnement, même si les positionnements politiques ne vont pas très loin.

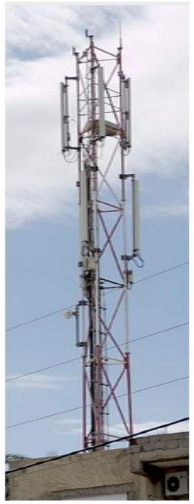
2 2 exemples : la collaboration de Google, Facebook, Twitter et Microsoft avec la commission européenne dans la lutte contre le terrorisme: https://www.laquadrature.net/2019/04/26/reglement-terroriste-premier-bilan-et-prochaines-etapes/, ceux-ci ont leur propre liste de personnes ou contenu « terroriste ». Ou sur le site transparency de google, on peut lire autour de 20 000 requêtes judiciaires par an par la france, dont 80 % amènent à des données envoyées

Quel est mon modèle de menace ?

Cette brochure essaye d'informer sur le fonctionnement des téléphones et des outils de surveillance de la police pour comprendre les enjeux et les choix de solutions. Cependant un certain nombre de choix nécessite d'avoir une réflexion sur un modèle de menace : contre qui je veux me protéger, quels sont leurs moyens et quelles ressources sont-ils prêts à mettre pour ces données, quels risques ces données font elles prendre s'ils ont accès à ces données. Des modèles de menace différents peuvent arriver à des solutions différentes. Il n'y a pas de solutions miracles, ni de planification de sécurité idéale déconnectée d'un contexte. Des choix ont été faits dans les propositions de cette brochure, qui peuvent être questionnés.

I) La téléphonie mobile et la sécurité

Les réseaux d'antennes téléphoniques [📞]



Le portable se connecte par ondes électromagnétiques à des antennes. L'antenne reconnaît alors la validité de la carte SIM et du téléphone. La carte SIM contient un numéro d'identification (IMSI) que l'opérateur vérifie afin d'autoriser ou non les communications avec d'autres téléphones.

Les antennes ne communiquent pas directement entre elles. Elles font le lien entre les téléphones et les serveurs de l'opérateur. Les communications sont transportées d'une antenne à l'autre par des câbles ou par des ondes. En plus de ces câbles et de ces ondes, nos communications passent par des ordinateurs (des routeurs et autres) qui acheminent le signal d'un endroit à un autre jusqu'à des nouvelles antennes et aux téléphones avec lesquels on communique.

Tout ce matériel réseau est possédé par des entreprises privées qui, comme toutes les boîtes, veulent se faire des sous ou avoir du pouvoir. Il n'est pas possible de faire confiance au matériel du réseau.

Les nouvelles technologies s'ajoutent aux anciennes, elles ne les remplacent pas. Les générations de technologies s'accumulent : en plus de la 4G et de la 5G (et d'ici peu de la 6G), il y a encore la 2G, 3G et d'autres, même s'il y a la volonté d'enlever la 2G un jour. Ces antennes sont présentes en ville, sur des immeubles, parfois cachées, sinon plus généralement sur des pylônes.

https://transparencyreport.google.com/user-data/overview.

6) Trucs techniques avancés / divers pour smartphone 📱

Cette section est plus développée sur https://telmob.0id.org/fr:divers.
Ces aspects ne sont potentiellement pas très accessibles sans un peu de compétences techniques, d'acharnement, ou de moyens financiers. Si des collectifs de geeks existent dans ton coin, ça vaut le coup de leur demander conseils.

Appli SnoopSnitch (Android)

SnoopSnitch analyse le micrologiciel de votre téléphone à la recherche de correctifs de sécurité Android installés ou manquants. Pour les Android « rootés », ce logiciel peut permettre de détecter les IMSI catcher.

Virer de force une application de surcouche

1) Applications Magisk et DeBloater

Magisk permet de passer en mode super-utilisateur (téléphone « rooté »), et **DeBloater** permet de virer les applications de force. Pratique pour les téléphones dont on ne peut pas changer l'OS.

2) Installer adb

adb est un petit logiciel qui permet de rentrer sur un téléphone dont le débogage USB est activé, d'accéder à la liste des applis installées, et d'en retirer de force.

Ça ne fonctionne pas à tous les coups.

Autres

- Gratter le numéro marqué sur la SIM (IMSI ou autre)
- Gratter celui ou ceux marqués sur le tél (IMEI, à l'intérieur)
- Installer un filtre de confidentialité. Il s'agit d'un film à mettre sur l'écran qui permet de rendre opaque ce qui se trouve sur l'écran quand on le regarde avec un angle de plus de 30°. Peut être intéressant pour l'usage du smartphone d'activités confidentielles dans un espace passant. Prix entre 10 et 20 euros en fonction des téléphones.

Autres systèmes d'exploitation

Quand on se procure un nouveau téléphone, si on a le choix, c'est bien de regarder si son modèle est compatible avec des systèmes d'exploitation alternatifs. Avec un *Ctrl+F*, on peut rapidement trouver des modèles qu'on convoite :

- **LineageOS** : https://wiki.lineageos.org/devices/
- **CarbonROM** : https://get.carbonrom.org/
- **/e/OS** : https://doc.e.foundation/devices

⚠ Installer un système d'exploitation alternatif est une opération complexe, et on peut rencontrer des problèmes non-évoqués dans les tutoriels. Si on veut le faire tout seul, le risque de le rendre totalement inutilisable (le « briquer ») est important, donc réfléchir à deux fois avant de cramer un billet dans le vent. Aussi avoir un système alternatif ne signifie pas forcément plus sécurisé face à la police.

Critères pour se procurer un téléphone sans pouvoir changer l'OS

Si on ne peut pas changer le système d'exploitation, on peut se baser sur des critères pour choisir un nouveau téléphone.

Parmi ces critères :

- l'année de fabrication / l'année prévue de fin des mises à jour ou correctifs de sécurité (https://endoflife.date)
- la version d'Android
- la marque du constructeur (certaines comme Xiaomi sont connues pour être très gourmandes en données personnelles)
- la possibilité de désactiver ou désinstaller les applications de surcouche de Google ou du constructeur
- la possibilité de changer les autorisations critiques sur les applications sur surcouche
- la possibilité de changer le système d'exploitation (voir partie précédente)

Si on se procure un téléphone d'occasion qu'on peut avoir en main avant de le choisir définitivement, c'est bien de le manipuler pour rapidement aller vérifier les différents critères : ⚙ **Paramètres → Système → À propos du téléphone**, et ⚙ **Paramètres → Applications → Gestionnaires d'autorisation** + voir si le bouton « désactiver » est cliquable pour des applications de base comme Photos, Fichiers, Horloge…

Les opérateurs communiquent entre eux afin qu'on puisse s'appeler depuis un compte chez Orange vers un compte chez Lyca par exemple, et vice-versa. Les opérateurs ont aussi des contrats avec des fournisseurs d'accès à internet, pour permettre l'accès internet sur les téléphones de leurs réseaux.

L'espace est découpé en cellule dans laquelle se trouve une antenne. Le passage d'une cellule à une autre nécessite d'être connectée à plusieurs antenne. Un téléphone essaie toujours de se connecter à plusieurs antennes afin de permettre de garder la communication. Quand on va dans un pays autre que celui où on a notre abonnement, on se connecte à des réseaux qui ont des contrats avec notre opérateur, ça s'appelle l'itinérance (ou le « roaming »).

Les enjeux spécifiques pour les téléphones portables 📱

Les téléphones sont fabriqués par des grosses entreprises capitalistes. Le matériel fabriqué n'est pas libre*, on ne sait pas la liste exacte des composants ni comment ça marche. Le nombre d'acteurs privés capables de construire ces différents composants sont peu nombreux, ce qui leur donne énormément de pouvoir.

Pour les **téléphones à boutons** de manière générale il n'y a pas de sécurité possible à espérer dessus. En effet : il n'y a pas de mise à jour possible, toute leur communication passe par un réseau non sécurisé. Il existe des téléphones à boutons avec des systèmes d'exploitation permettant de les chiffrer ou d'utiliser quelques applications sécurisées[3] telles que signal , dans ce cas on trouve les mêmes problématiques que les smartphones.

Les téléphones dits « intelligents » ou **smartphones** font ce pourquoi ils ont été fabriqués et rien de plus. Ils ne sont pas intelligents ! En réalité il s'agit du même outil qu'un téléphone à boutons : c'est un petit ordinateur. Seulement le smartphone est plus puissant et contient plein de capteurs : de quoi mesurer les vitesses de déplacement, d'accélération, le rythme cardiaque (ce capteur qui permet de calculer le rythme cardiaque est tellement puissant qu'il pourrait en théorie reconstituer le son à partir des vibrations même si le micro est fermé), la luminosité ambiante, caméras, gyroscope, magnétomètre… De nombreux smartphones sont aussi puissants qu'un ordinateur milieu de gamme, voire plus.

3 On peut trouver des marques sur ce site internet : https://dumbphones.pory.app/

Vue éclatée d'un smartphone avec ses différents composants.

Les téléphones ont des problématiques spécifiques de sécurité numérique :

- Ils sont [*pour la plupart des usager·es*] toujours allumés avec **énormément de données dedans** dont une partie qu'on n'a pas décidé d'avoir.
- Y a **pas de normes matérielles** sur les téléphones portables. Les fabricants de téléphones [Samsung, Google, Apple, etc.] achètent les différents composants (écran, GSM, carte wifi, batterie, etc.) et assemblent le tout. Dans les ordis, il y a beaucoup plus de normalisation et de compatibilité des composants entre les différents modèles et marques. Ces composants spécifiques à chaque modèle de téléphone rend plus compliqué d'avoir des systèmes d'exploitation alternatifs (plus sécurisés que celui installé à l'origine ou avec une idéologie moins douteuse, par exemple). Le matériel est fabriqué par des entreprises privées soumises aux réglementations étatiques. Les téléphones sont fournis avec des logiciels propriétaires*, il y a peu de volonté en termes de sécurité, et peu de documentation publique.
- Les smartphones comportent plusieurs **couches logicielles**, chacune ayant des problématiques de sécurité différentes :

5) Changer de système d'exploitation

⇒ Nécessite d'avoir un téléphone compatible (liste disponible sur les sites respectifs des systèmes d'exploitation)
⇒ Attention, ça ne résout pas les problèmes inévitables, et surtout libre ne signifie pas sécurisé face à la police ![29]
⇒ Système d'exploitation libre* existant : **LineageOS**[30], **GrapheneOS**, **CarbonROM**, **/e/**[31], etc. ⚠ La plupart sont très compliqués à installer / mettre en œuvre et doit être fait avec des personnes ayant des compétences avancées.

Se procurer un téléphone Pixel et installer GrapheneOS

GrapheneOS est un système d'exploitation mobile libre axé sur la sécurité et la confidentialité en compatibilité avec les applications classiques d'Android. C'est le système d'exploitation le plus fiable en termes de sécurité numérique à ce jour et il est plutôt facile à installer. Cependant, il n'est compatible qu'avec les téléphones Google Pixel. Attention les versions antérieures à Pixel 6 ont un soucis de sécurité[32] Il faut prendre au-dessus du 6a. Au dessus de ce modèle, UFED n'est pas en capacité de tester des milliards de mot de passe sur le téléphone, ce qui protège son chiffrement. Les Pixel 8 et 9 présentent l'avantage de sécurité d'être développés jusqu'au moins 2030 et d'une puce particulièrement sécurisée dont **GrapheneOS** fait un usage de qualité.

Pour installer **GrapheneOS** sur son Pixel, le mode d'installation est bien plus accessible que les autres systèmes d'exploitation mobile, il faut suivre les instructions qu'il y a sur leur site (grapheneos.org/install/web), qui n'est cependant disponible qu'en anglais.

> (i) Les informations du collectif **Technopolice Belgique** sur les systèmes d'exploitations téléphoniques en termes de sécurité, avec leur durée de développement en fonction du téléphone sont trouvables ici : technopolice.be/smartphones/

29 Pour des comparaisons de système d'exploitation de téléphone en terme de sécurité, voir ici (infos en anglais et technique) : https://eylenburg.github.io/android_comparison.htm
30 Un très bon tutoriel explicatif de pourquoi et comment installer **LineageOS** sur smartphone est disponible à cette page : https://linuxfr.org/news/installer-lineageos-sur-son-appareil-android
31 Modèles de téléphones disponible : https://divestos.org/index.php?page=devices&base=LineageOS
32 Les versions avant Pixel 6 peuvent subir du brute force par le logiciel Cellebrite: https://next.ink/144397/tentative-dassassinat-de-trump-cellebrite-deverrouille-un-samsung-mais-peine-avec-apple-et-google/

1) Tu récupères une nouvelle carte SIM, et tu payes ton crédit en liquide dans un bureau de tabac ou un magasin Lyca, pour remplir le forfait de ton téléphone.

2) La première fois tu dois enregistrer ton téléphone : soit par téléphone, soit par internet. À chaque fois des données personnelles te seront demandées mais tu peux donner des informations fantaisistes, il n'y a pas de vérifications. Si on te demande une photocopie de carte d'identité, tu peux mettre un faux ou une photo de montagne, ça marche (à vérifier par opérateur), et si on te demande le numéro de ta carte d'identité tu dis le bon nombre de numéro mais tu les changes. Tu peux t'aider de dcode.fr/carte-identite-francaise pour trouver un numéro crédible.

Parfois, il faut un peu de temps (quelques heures) avant que ça soit effectif, c'est bien de préparer le téléphone à l'avance. Tu mets ensuite un code pour avoir un forfait. Par exemple tu peux très bien entrer 40 euros de crédit achetés dans un bureau de tabac, et avec le code il va te débiter chaque mois une partie du crédit jusqu'à ce qu'il n'y a plus assez (dans ce cas il faudra rentrer à nouveau du crédit).

Des fois faut chercher les meilleures offres. Pour **Lycamobile** par exemple, il faut taper *139*3004# pour avoir un forfait 5 euros par mois, téléphone et SMS illimité mais pas d'internet, et *139*4099# pour avoir 10 euros d'illimité et un peu de forfait internet.

Petits tips à faire attention :

- Une ligne avec 0 € de forfait qui n'est pas utilisée pendant plusieurs mois peut être coupée. Penser à vérifier son crédit de temps en temps et à remettre des sous si on est à 0 €.
- Ne pas utiliser une carte SIM qui a été utilisée auparavant sous une identité qui t'es liée, ne pas mettre ta nouvelle carte SIM dans un téléphone déjà utilisé dans le passé lié à une identité.
- En cas de recherche, la police peut savoir dans quel point de vente a été acheté le forfait.
- Réfléchir au niveau d'anonymat que l'on veut. C'est déjà important et pas inutile d'avoir un téléphone qui n'est pas relié à ton identité car les recherches premières des flics se limiteront à faire une requête aux opérateurs pour connaître l'identité des personnes derrière un numéro IMSI ou IMEI. Ils peuvent mettre en place d'autres méthodes pour savoir qui est derrière un téléphone (mise sous écoute, étude des numéros contactés avec le téléphone, IMSI-catcher, etc), ou peuvent mettre sous écoute tes proches pour trouver ton nouveau numéro lorsque tu les appelleras. Mais ça demande plus de moyens, donc ça dépend du modèle de menace.
- Inviter à ce qu'il y ait plus de gens à utiliser ces techniques, c'est se protéger dans la masse. Si, dans une manif, il n'y a qu'un téléphone d'une carte prépayée qui borne, il pourrait paraître suspect en cas d'enquête.

1. **Les pilotes des différents composants du téléphone :**

   Ce sont les logiciels qui permettent que les composants fonctionnent (écran, micro, antennes, gyroscope, etc.). Ils sont fournis par les différents constructeurs des composants, non-documentés publiquement.

2. **Le système d'exploitation installé sur le smartphone :**

   Le système d'exploitation c'est l'ensemble des logiciels qui fait marcher le téléphone (ou l'ordi). On voit cela par la suite.

3. **Les applications installées par défaut**

   Les applications d'Apple, de Google, ou du constructeur, sont parfois compliquées à désactiver et souvent impossibles à désinstaller si on n'a pas de compétences techniques. Certaines ne peuvent pas être retirées sans créer des bugs sur le smartphone.

4. **Les applications qu'on installe :**

- Trouvées sur les magasins d'applications (AppStore, Google Store, F-Droid, etc.), plus ou moins open-source, plus ou moins malveillantes selon les permissions qu'elles demandent.
- Les applications fonctionnent avec des **permissions d'accès** au téléphone. Que ce soit dans Android ou iOS, chaque application se donne des droits d'accès à ton téléphone. En tout et selon le modèle de l'appareil, il y a plus de 300 autorisations possibles (aussi appelées permissions), le Play Store de Google par exemple en demande 133, Facebook en demande 85. Il y a les **autorisations sensibles** (accès à tous les fichiers du tél, micro, caméra, etc.), les **autorisations spéciales** (installation d'applications de sources inconnues, accès aux données d'utilisation, accès à la liste des applications installées, espécialestc.) et les **autorisations communes** (orientation de l'écran, détection des captures d'écran, accès à Internet, vibreur, etc.). C'est le constructeur ou le développeur du système d'exploitation qui détermine ce qui est sensible ou non et on ne peut pas faire confiance à la majorité d'entre eux.

  Il est possible d'afficher et de modifier les permissions de chaque application (sur Android : ⚙ Paramètres → Stockage → Applications installées ; sur iOS : Réglages > Confidentialité et sécurité ; on peut retrouver les différentes catégories de permissions). Certaines applis peuvent demander des permissions qui ne sont pas nécessaires à leur fonctionnement, dans l'intention de récolter des données supplémentaires. L'application Exodus Privacy (sous Android) permet d'afficher les pisteurs et les autorisations de chaque application

Tableau de permissions possibles sur android :

- **Agenda** : Lire / modifier / créer des évènements dans l'agenda.
- **Journaux d'appels** : consulter et modifier l'historique de vos appels.
- **Appareil photo** : utiliser votre caméra pour prendre des photos ou enregistrer des vidéos.
- **Micro** : utiliser le microphone pour prendre du son.
- **Contacts** : accéder à votre liste de contacts / la modifier.
- **Position** : obtenir la position (approximative par GSM ou wifi, ou exact par gps) de votre appareil.
-
- **Appareils Bluetooth à proximité** : les applications peuvent détecter les appareils à proximité et s'y connecter.
- **Téléphone** : passer et gérer des appels téléphoniques, lire le statut du téléphone, la liste des appels, voir qui appelle, modifier la liste des appels, ajouter des messageries vocales, utiliser la VoIP (voix par internet), rediriger / suspendre des appels,....
- **Activité physique** : obtenir des informations sur votre activité physique (marche, vélo, nombre de pas, etc.).
- **Capteurs corporels** : obtenir des informations sur vos signes vitaux.
- **SMS** : accéder aux SMS entrants et envoyer des SMS.
- **Stockage** : Gestion des modes de stockage des données et des accès des applis.

Aussi :
- Si les applications capitalistes sont gratuites, c'est que pour beaucoup leur modèle économique est basé sur le vol et la revente des données personnelles qu'on leur fournit par notre usage.
- Accéder gratuitement à des logiciels payants peut amener à nous faire installer un logiciel malveillant (aussi appelées malwares) en parallèle de l'appli sans qu'on s'en rende compte. Ça ne va pas forcément donner des infos aux keufs, plutôt à des groupes qui vont revendre les infos pour faire de la maille, mais certains services de police ou de renseignement peuvent aussi acheter des données sur les marchés privés

Lien entre les applications / identifiant publicitaire 📱

Les smartphones récents essayent de séparer les applis pour qu'ils ne puissent pas extraire des données des autres ou qu'il y ait de liens entre plusieurs applis (pour par exemple identifier plusieurs usages d'une personne, la suivre à la trace, etc.). Cependant :

Wifi, accès à tous les fichiers (sauf Gestionnaire de fichiers / Galerie) ; modification des paramètres système.

Concernant les **communes** : on ne peut rien faire.

Paramétrages généraux sous Android

• Mode USB par défaut : charge uniquement
• Avoir un modèle de téléphone qui présente encore des MAJ de sécurité (vérifier les dates sur endoflife.date/pixel et autres pages spécifiques de téléphones)
• Mettre un verrouillage d'écran rapide + un bon code de déverrouillage
• Désactiver l'identifiant de publicité ciblée qui récolte des données personnelles soit dans ⚙ **Paramètres → Google → Annonces soit dans ⚙ Paramètres → Confidentialité → Publicités**
• Chiffrement du téléphone (il est activé par défaut depuis Android 10)
• Notifications discrètes
• Suspendre l'activité et les autorisations des applis non-utilisées pendant plusieurs mois (voir dans le gestionnaire d'autorisations, pour chaque application)
• Utiliser les **Profils / Comptes d'Utilisateurs** pour séparer certains usages (militant/perso/pro), ou l'isolement d'applis à l'aide de **Shelter**..
• Ne pas désactiver l'application « **Google Play Services** » sinon ça peut entraîner des dysfonctionnements importants

Paramétrages généraux sous iOS

• Code de déverrouillage
• Désactiver les sauvegardes sur **iCloud**
• Désactiver l'identifiant de publicité
• Attention aux notifications
• Activer l'**USB Restricted Mode** (cette option bloque tout échange de données si l'appareil n'a pas été déverrouillé depuis 1h)
• Activer la réinitialisation automatique du téléphone après 10 tentatives de déverrouillage infructueuses (⚠ toutes les données du téléphones sont perdues définitivement)
• Activer le mode isolement / **Lockdown Mode**
• Chercher des versions iOS des applications listées plus haut
⇒ Le téléphone est chiffré* par défaut, mais parfois ce chiffrement est contournable.

4) Avoir un téléphone dont la carte SIM est « anonyme » [📞]

Il est possible d'avoir un téléphone « anonyme » en utilisant les cartes prépayées. On peut retrouver plusieurs marques : **Lycamobile**, **Lebara**, **Syma** (d'autres opérateurs en proposent, à tester).

aléatoires (ou de 25 chiffres aléatoires pour une force équivalente). Sur un système qui n'est plus mis à jour, il faut partir du principe que même un mot de passe long n'est pas une garantie suffisante contre un UFED (mais ça vaut le coup d'essayer).

Le problème c'est que le code de chiffrement est le même que le code de déverrouillage de l'écran (sauf sous **GrapheneOS** où c'est possible d'en avoir 2 séparés), ce qui amène beaucoup de monde à faire des codes plus courts, car il faut le taper souvent, ce qui n'est pas compatible avec une bonne sécurité face à des moyens d'enquête poussés.

Si tu veux sauvegarder ton code quelque part, le mieux est d'utiliser un coffre fort à mot de passe comme **KeePassXC** sur ordi ou **KeePassDX** sur téléphone, si tu l'oublies souvent tu peux demander à des personnes dans ton entourage en qui t'as confiance pour le stocker.

Réseau et chiffrement des communications

Au niveau du réseau, il vaut mieux chiffrer ses communications de bout en bout (voir conseils d'applis) pour que le contenu ne soit pas divulgué, et pour cacher les sites internets fréquentés faire passer les applications par un **VPN** ou par le réseau **Tor**.

Activer la fonctionnalité « killswitch VPN ». Cette fonctionnalité permet d'éviter les fuites si le VPN est déconnecté. Elle se trouve dans ⚙ **Paramètres → Réseau et internet → VPN →** ⚙ **→ Bloquer les connexions sans VPN.**

Désactiver les fonctionnalités non-utilisées

Quand c'est possible, désactiver les services Bluetooth et de localisation. Il y a parfois des interrupteurs à bascule pour l'appareil photo et le microphone. Lorsque vous ne les utilisez pas, il est mieux de désactiver ces fonctionnalités. Les applications ne peuvent pas utiliser les fonctions désactivées (même si elles ont reçu une autorisation individuelle) tant qu'elles ne sont pas réactivées.

Gérer les autorisations

Sous Android, il est important de vérifier les permissions d'une application. Il existe 3 types d'autorisations (voir plus haut) : les sensibles, les spéciales et les communes. Pour trouver les **sensibles** : ⚙ **Paramètres → Applications → Gestionnaire d'autorisations** ou ⚙ **Paramètres → Confidentialité → Gestionnaires d'autorisation**. Réfléchir à chaque application si elle a réellement besoin de cette permission (Agenda, appareil photo, contacts…).

Pour les **spéciales** : ⚙ **Paramètres → Applications → Accès spéciaux des applications** ou **Autorisations spécifiques des applications**. Les autorisations spéciales critiques à désactiver : accès aux données d'utilisation ; installation d'applications de sources inconnues (sauf pour les magasins d'app) ; contrôle du

- De nombreuses applis très connues utilisent des **pisteurs (ou trackers)** pour récupérer des infos supplémentaires. Un pisteur permet la collecte de données sur l'usage du téléphone ou sur l'utilisateur. Par exemple, jusqu'à juin 2025, en ouvrant l'appli Facebook ou Instagram, on ouvrait en même temps un service en arrière plan. Celui-ci faisait lien entre le compte personnel Facebook et les sites web ouverts sur un navigateur web qui possèdent un mouchard Facebook (beaucoup de sites internet)[4]. Pour limiter les risques, il est mieux si possible d'utiliser certains services sur un navigateur internet plutôt qu'installer l'appli du même service, ou de questionner quel service on veut utiliser. Certains systèmes d'exploitation permettent de séparer les identités de manière plus stricte sur un smartphone (voir dans la suite de la brochure).
- Il existe un **identifiant publicitaire**[5], qui est un identifiant unique faisant lien entre les applications. Il est notamment utilisé pour que certaines entreprises nous suivent à la trace en récoltant des données de localisation de plusieurs applications, ou encore de nous identifier de manière unique d'une appli à une autre.

Le système d'exploitation du smartphone 📱

C'est le gros logiciel qui permet au autres logiciels de fonctionner (pilotes matériels, applications) et de s'afficher.

Il en existe un certain nombre : Android, iOS, Windows, GrapheneOS, Blackberry, Ubuntu Touch, /e/, LineageOS, etc. En termes de sécurité, le mieux est **GrapheneOS** mais ne s'installe que sur des Pixel (voir chapitre *changer de système*

4 Lire « Meta et Yandex traquaient la navigation des utilisateurs d'Android via leurs applications », juin 2025, sur next.ink, ou l'article en anglais plus complet sur arstechnica : https://arstechnica.com/security/2025/06/meta-and-yandex-are-de-anonymizing-android-users-web-browsing-identifiers/

5 « *Les identifiants publicitaires sont des identifiants numériques, souvent représentés sous forme de chaînes de caractères, générés et associés à un terminal par l'OS, et qui peuvent, sous certaines conditions dépendantes de l'OS en question, être mises à disposition des applications qui en font la demande. Ces identifiants sont spécifiquement conçus pour permettre l'identification d'un unique utilisateur par différentes applications, identification rendue en dehors de celui-ci impossible par l'exécution en mode « bac à sable » (« sandboxing ») des applications. Cette identification permet notamment le ciblage publicitaire. Par exemple, si un utilisateur est connecté sur un réseau social depuis son téléphone et que des applications tierces embarquent le module de ciblage de ce réseau social, l'accès à l'identifiant publicitaire permettra d'utiliser les données relatives au profil de la personne pour cibler de la publicité dans le contexte de ces applications tierces.* » Définition de la CNIL

d'exploitation). Attention, un système libre ou alternatif ne veut pas dire sécurisé. On va s'attarder ici sur les 2 principaux utilisés.

Problématiques spécifiques des 2 systèmes d'exploitation principaux sur smartphone

Apple

Ecosystème où la marque contrôle tout. C'est les ingénieurs Apple qui font iOS (le système d'exploitation) et qui conçoivent les téléphones, les commerciaux Apple qui les diffusent, et les magasins Apple qui les vendent et les réparent. Apple contrôle tout, de la conception à la commercialisation, aux mises à jour, à l'après-vente…

Problématique : Ce système d'exploitation ainsi que ses applications sont propriétaires*.

Avantages : les mises à jour du système sont suivies plus longtemps, le matériel est de bonne qualité, le système est cohérent et fonctionne bien. Éteint, le chiffrement des appareils récents (à partir des iPhones 12) est costaud contre les outils de la police (protégé contre les UFED)[6].

Android

Le système d'exploitation Android (AOSP) a été racheté en 2005 par Google. Elle a une base open-source pour pouvoir bénéficier du travail gratos de développeur·ses qui font leurs propres versions et contribuent à son amélioration.

- Lorsque l'AOSP est repris par les constructeurs de téléphones, Google y impose au passage ses applications (Play Store, Play Services, clavier Gboard, Photos, Drive, etc.), propriétaires*. Le déploiement d'Android par Google à l'échelle planétaire est tel qu'il est dans une situation de quasi-monopole (hors-Apple).
- Les constructeurs (Samsung, Xiaomi, Sony, Nokia, etc.) peuvent le modifier pour ajouter leurs fonctionnalités et surcouches (MiUI, One UI, Samsung Galaxy Store, etc.).
- Il y a des morceaux de logiciels des fabricants de composants (souvent propriétaires*), comme les pilotes wifi ou d'autres trucs.
- Les opérateurs téléphoniques rajoutent aussi parfois une surcouche, comme Orange Music, SFR & Moi, ou autre.

6 Informations datant d'avril 2024 et concernant les iOS 17.4

Plus d'informations sur le site de l'application[28].

Session

Session est un fork* de **Signal** qui a créé son propre protocole de communication, pour le rendre non-centralisé. Ça veut dire que tous les messages ne doivent pas nécessairement passer par les serveurs de l'application mais l'ensemble des serveurs qui hébergent les utilisateur·rices. Cependant, **Session** base son réseau sur **Lokinet**, qui dépend de la blockchain, et beaucoup préféreront rester éloigné·es de ça, parce que cette technologie trouve ses bases dans l'idéologie libertarienne (un capitalisme certain opposé à toute forme de régulation).

3) Paramètres du smartphone 📱

La majorité des paramètres cités ci-dessous peut être trouvée en tapant des mots-clés dans la barre de recherche des ⚙ **Paramètres**. Il est possible que le chemin pour accéder aux paramètres spécifiques soit différent de celui indiqué ici.

Un bon code de chiffrement du téléphone

On va éviter la reconnaissance faciale (problématique en tant que technologie et y a des failles). Sur le déverrouillage de type « schéma », souvent il reste des traces sur l'écran qui permet de les déduire.

Les empreintes digitales peuvent être une forte défense face à des téléphones dont le mot de passe peut être testé en *bruteforce*, mais ne protège pas qu'on soit contraint de mettre son doigt, ou d'une reconstitution de l'empreinte.

Opter pour une **phrase de passe** est mieux en termes de sécurité mais ça peut devenir pénible à taper (adapter le temps de verrouillage de l'écran).

Pour des modèles de menace avec peu de risque d'enquête policière, opter pour un **digicode** est bien à condition d'en avoir un assez long (12-14 chiffres ou plus). C'est encore mieux si on active l'option « disposition aléatoire » des chiffres disponible sur certains systèmes.Mais dans certaines activités militantes, le digicode est très vite dangereux.

Un bon mot de passe dépend de son ***modèle de menace*** (voir plus haut) ainsi que du système d'exploitation qu'on utilise. **Penser à éteindre un téléphone chiffré avant saisie pour activer le chiffrement**.

S'il y a des risques d'enquêtes policières approfondies avec des moyens financiers, pour des **Pixel** récents (après le 6a) sous **GrapheneOS**, un mot de passe digicode de 10 chiffres sur une disposition aléatoire peut être suffisant. Pour des téléphones qui ne sont pas sous **GrapheneOS**, envisager un mot de passe long d'au moins 16 caractères aléatoires (avec lettre majuscule / minuscules) ou d'au moins 6 mots

28 https://molly.im/

(i) **Tutoriel -** Quelques configurations de Signal avec des impressions d'écran sur le site de Surveillance Self-Defense : ssd.eff.org/fr/module/guide-pratique-utiliser-signal

Avoir Signal sur ordinateur

Il est possible d'installer **signal-desktop** sur ordinateur quel que soit le système d'exploitation. Il faut scanner le QR à partir d'un smartphone et activer de temps en temps le téléphone, mais ça peut permettre de consulter ses signal dans certains lieux sans avoir à borner avec le téléphone. On peut aussi utiliser un smartphone en mode avion connecté par wifi, mais il est plus compliqué techniquement de ne pas relier le téléphone à la box ou au partage de connexion.

Il est aussi possible d'utiliser **Signal** sur ordi sans smartphone avec un téléphone à touche grâce à **signal-cli**. Il peut aussi y avoir plusieurs comptes **Signal** sur un ordi. Ces deux possibilités sont techniques à mettre initialement en place, il vaut mieux être accompagné.e pour cela. Il y a cette outils, signal tools[27] qui intègre cela et bien d'autres outils.

Utiliser Signal sans Signal

Signal est une application qui n'est que partiellement libre* (open-source et dont la reproduction, la modification et la diffusion sont libres). Certaines parties du code de **Signal** utilisent des morceaux de code de Google qui sont propriétaires (l'inverse de libre).

Il existe des applications qui reprennent le code-source de **Signal** pour en modifier les parties libres. Le protocole d'échange étant le même, il est possible d'échanger un message **Signal** depuis une de ces applications alternatives.

Molly et Molly-FOSS

Comme **Signal**, **Molly** utilise les parties de code propriétaires issues de Google. Cependant, **Molly** propose quelques options que **Signal** n'a pas :

- avoir un code de déverrouillage de l'application différent du code utilisé pour verrouiller le téléphone

- programmer des sauvegardes

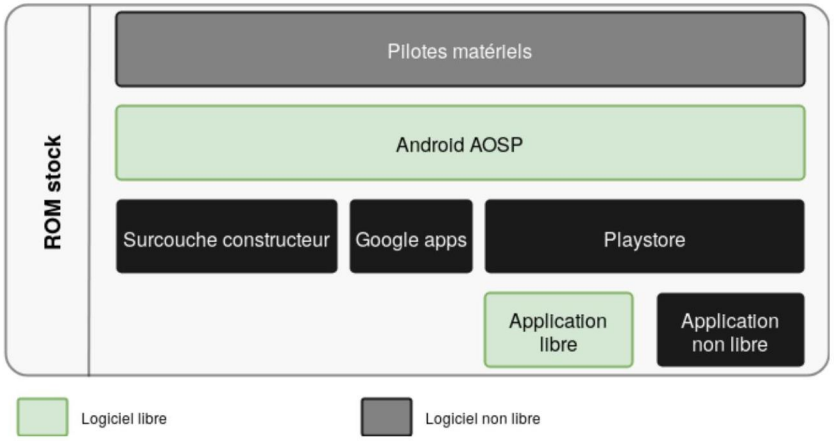
- forcer l'utilisation d'un VPN pour son fonctionnement

Molly-FOSS est une tentative de la communauté autour de Molly de rendre l'application 100 % libre, donc proposer une application qui soit libérée des morceaux de code appartenant à Google.

27 https://0xacab.org/TheCodesUprising/tools/signal-tools

Lorsqu'un des acteurs arrêtent de développer son composant, les mises à jours du smartphone devient impossible. Beaucoup de téléphones sous Android n'ont plus de mises à jour rapidement après leur lancement. Cela signifie que les failles de sécurité découvertes dans le temps ne sont pas corrigées.

Architecture d'un téléphone sous Android



II) Les problèmes inévitables de sécurité dans les téléphones [ ]

Ce qu'on ne peut pas actuellement résoudre avec les téléphones :

Géolocalisation du téléphone [ ]

Un téléphone allumé (même sans carte SIM) est géolocalisable très simplement par les entreprises qui contrôlent les antennes (et donc les keufs peuvent leur demander certaines infos). Il y a plusieurs sources de géolocalisation du téléphone, dont certaines sont indépendantes de si l'option localisation est allumée ou non.

Différents types de localisation par smartphone

Le fonctionnement du GPS : Les satellites émettent leur positionnement. Activer la localisation, c'est demander au téléphone de capter ces signaux et ainsi savoir avec précision où il se situe (être sous terre ou dans un bâtiment peut fausser ou rendre impossible la localisation). Les applications peuvent récupérer cette localisation qui a une précision de quelques mètres, mais les satellites n'ont pas connaissance de la localisation des appareils.

Antennes téléphoniques (2G, 3G, 4G, 5G) : le téléphone et les antennes sont continuellement en communication, dès lors que ce premier est allumé (et pas en mode avion, carte SIM ou pas). Les antennes ont connaissance de la distance à laquelle se trouve un téléphone, donc un rayon autour de l'antenne. Une « triangulation » avec 3 antennes permet une localisation. Sans cette triangulation, la précision est faible (plusieurs centaines de mètres).

Localisation par wifi : le téléphone est localisé par la position connue des réseaux wifi par 2 techniques différentes :

- L'une se base sur le partage des réseaux wifi environnants, détectés par l'appareil et pas seulement le réseaux wifi auquel on est connecté·e, pour nous placer dans l'espace (utilisé notamment par Google Maps en plus du GPS ou des antennes téléphoniques).
- L'autre utilise l'adresse MAC du téléphone qui jusqu'à récemment était fixe (possiblement aléatoire depuis Android 11, et depuis iOS 14) pour l'identifier lorsqu'il se connecte à plusieurs réseaux wifi à la suite[7].

7 Cela était notamment utilisé par des "poubelles intelligentes" au royaume-Unis pour suivre les personnes à la trace (https://arstechnica.com/information-technology/2013/08/no-this-isnt-a-scene-from-minority-report-this-trash-can-is-stalking-you/)

PARAMÈTRES/COMPTE (important)

- Mettre un NIP (⚠ lire la notice) et activer blocage d'inscription.

PARAMÈTRES/CONFIDENTIALITÉ

- Numéro de téléphone : « Qui peut voir mon numéro » : personne (par défaut).
-
- Activer les messages éphémères et mettre une valeur par défaut (ex : 1 semaine).
- Activer la sécurité d'écran (verrou d'écran) : pour ouvrir l'application il faut remettre son code de déverrouillage de téléphone.
- Activer un verrouillage automatique de l'écran avec un temps qui correspond à son modèle de menace (et prendre l'habitude de le modifier selon les contextes) : c'est le temps que met le téléphone à reverrouiller l'application.
- Activer l'option « Clavier incognito »
- Activer la sécurité de l'écran (empêche les captures d'écran pour soi-même = si quelqu'un prend le téléphone, il ne peut pas rapidement faire une capture et se l'envoyer + ça permet d'éviter que le contenu de Signal n'en sorte et se balade dans les dossiers d'images de son téléphone)

PARAMÈTRES/CONFIDENTIALITÉ/PARAMÈTRES AVANCÉS

- Activer l'option « Toujours relayer les appels » (important de comprendre les implications : ça permet de ne pas divulguer l'adresse IP de notre connexion aux destinataires de nos appels)

PARAMÈTRES/APPAREILS ASSOCIÉS

- Vérifier les appareils associés régulièrement (si Signal a été installé sur un ordinateur ou un autre téléphone, il s'affiche dans la liste des appareils reliés)

AUTRES

- Numéro de sécurité à vérifier avec ses correspondant·es (flasher un QR code sur le téléphone de son contact quand on le croise en vrai)

(i) Une liste détaillée (et fréquemment mise à jour) des paramètres est inscrite sur le wiki Téléphonie mobile & Activisme (telmob.0id.org/fr:signal).

En cas de réquisition judiciaire faite à Signal, Signal promet ne posséder que la date de création du compte ainsi que la date de la dernière connexion au compte : sur leur site on peut retrouver ce que Signal dit fournir aux institutions judiciaires : https://signal.org/bigbrother/.

les profils et n'utiliser Aurora Store (et des outils Google) que dans un profil dédié. Par exemple, on peut imaginer un compte avec l'usage des outils propriétaires ou des GAFAM, et un compte avec des outils militants[26].

Autres

Une bonne série d'applications dispo dans F-Droid : Fossify (fossify.org). Il y a un calendrier, un gestionnaire de fichiers, un gestionnaire de contacts, une appli de SMS, des notes, un enregistreur vocal, etc.

Un certain nombre d'apps ont des versions ordinateurs – à prendre en considération pour avoir des communications ordi-téléphones :

- Signal (Signal-desktop, axolotl.chat)
- Conversations, compatible avec Dino, Pidgin, Gajim, etc
- Element (https://element.io/get-started)
- Thunderbirdetc.

Revenons sur Signal / Molly

Défauts

- Possible sensation de sécurité parfaite, illusoire
- Centralisé : protocole utilisable uniquement sur cette application ou ses forks* et sur leur serveur
- Pour s'inscrire, il faut le lier à un numéro de téléphone souvent relié à une identité réelle (même s'il n'est pas visible pour les utilisateur·ices)
- Idéologies cheloues (intégration de cryptomonnaie, refus de décentraliser…)
- Modèle économique douteux : certain·es développeur·euses sont payé·es 600 000 dollars par an ; l'application n'est pas rentable, est en déficit et reçoit des apports d'argent douteux ; double discours en fonction de si Signal s'adresse à ses investisseurs ou à son public.

Options à configurer dans Signal

PARAMÈTRES/PROFIL (important) :

- Nom ; À propos ; Photo de profil → rester anonyme le plus possible.
- Ajouter un nom d'utilisateur.ice (@XXXXX.NN), se terminant nécessairement par un point et 2 chiffres. Cet identifiant permettra d'être retrouvé·e sur Signal par les autres utilisateur·rices. Il n'est pas visible par défaut, il faut penser à le demander ou l'envoyer pour mettre en lien des personnes par Signal. On peut aussi le mettre en description ("À propos") pour que nos contacts l'aient rapidement.

26 Le guide « GrapheneOS for Anarchists » sur anarsec.guide explique pourquoi et comment avoir une utilisation optimale des Profils d'utilisateur

TECHNOLOGIE	PRECISION DE GEOLOCALISATION
GSM (2G)	Environ 200 à 1000 mètres
UMTS (3G)	Environ 50 à 300 mètres
LTE (4G)	Environ 5 à 50 mètres
5G	Environ 1 à 10 mètres
GPS	Environ 5 à 10 mètres (en plein air)

Précision de géolocalisation en fonction de la technologie. Cette précision dépend du terrain et du nombre d'antennes sur le territoire.

Le mode avion coupe toute connexion aux antennes, donc la localisation par l'opérateur devient impossible.

Appels et SMS en clair [ ]

Les appels et SMS qu'on envoie passent en clair* dans le réseau. C'est-à-dire que leur contenu ainsi que les métadonnées* les concernant sont interceptables. Dans la réalité, c'est un peu plus compliqué car les communications ont un chiffrement, mais ce chiffrement est fait pour être désactivable par des acteur·ices étatiques. Que ce soit en 2G, 3G, 4G, ou 5G.

Il est fourni aux enquêteurs des outils qui permettent très facilement et automatiquement d'exploiter les métadonnées (heure/date d'un SMS, destinataire, antenne concernée…).. En plus de pouvoir identifier une personne ou ses comportements, ça leur permet aussi de faire des graphes relationnels, de savoir qui est « au centre » d'un groupe, etc. De plus, les métadonnées des conversations sont disponibles légalement de manière rétro-actives mais pas leur contenu : en france, le délai minimum légal de leur conservation est d'1 an. Cependant si ces données ont été demandées dans une enquête dans l'année, elles peuvent être utilisées plus longuement dans le temps.

Conditions pour que le téléphone ne communique plus avec les antennes

En mode avion, les téléphones ne communiquent plus avec les antennes et donc il n'y a pas de géolocalisation possible de la part des antennes. Cependant, on peut imaginer des logiciels malveillants qui récolteraient la géolocalisation via le GPS et la transmettraient lorsque le téléphone se reconnecte au réseau. On peut aussi retirer la carte SIM pour diminuer le risque de connexion par mauvaise manipulation (oups j'ai désactivé le mode avion).

Éteint, le téléphone ne communique pas avec les antennes. Cependant, il peut parfois se rallumer, par exemple certains téléphones s'allument quand un réveil se déclenche. Ou notre poche peut appuyer sur le bouton d'alimentation… Même si ça ne semble pas être fréquent, pour se protéger de cela, le top est d'enlever la batterie. La plupart des modèles de smartphones ne permettent pas d'enlever la batterie. On peut aussi enrouler le tel dans une quinzaine de couches d'alu alimentaire, histoire de bien l'isoler des ondes.

Un téléphone allumé sans carte SIM peut techniquement se connecter au réseau téléphonique avec son IMEI (voir paragraphe suivant). En france, la fonction « appels d'urgence » sans carte SIM a cependant été désactivée par l'État.

Identification des téléphones [ ]

IMEI / IMSI

Lorsque le téléphone se connecte à une antenne, il transmet les **identifiants IMSI** des cartes SIM actives, les identifiants IMEI du téléphone, le modèle du téléphone et l'opérateur téléphonique utilisé. L'IMSI (pour « Identifiant d'abonné·e mobile international ») est l'un des identifiants permettant à l'opérateur de vérifier que la carte SIM a le droit de communiquer sur son réseau.

Le **numéro IMEI** (pour « identifiant d'équipement mobile international ») est un identifiant unique par emplacement de carte SIM de chaque téléphone. Il est lié à la marque de l'appareil ainsi qu'au modèle précis, parfois même à la couleur de la coque. C'est lui qui sert à bloquer un téléphone quand il est déclaré volé (même si c'est rarement mis en place).

Cet identifiant est stocké de manière définitive dans le téléphone. On ne peut pas modifier (« usurper ») l'identifiant IMEI d'un téléphone (enfin c'est *presque* impossible, bien que des possibilités commencent à voir le jour). On peut connaître les numéros IMEI d'un tel en composant le *#06#. L'IMEI est une suite de 15 à 17 chiffres qui comprend :

- Les deux premiers chiffres indiquent le pays de fabrication
- Les six chiffres suivants représentent le numéro de série
- Le dernier chiffre est un chiffre d'authentification et sert donc de clé de sécurité.

En france, les opérateurs gardent les infos de connexion pendant 1 an. Ça veut dire que l'information précisant quel IMSI était dans quel IMEI est gardée tout ce temps. Avec ça est aussi gardée la liste des antennes auxquelles s'est connecté un téléphone ainsi que les dates et heures correspondantes. D'autres infos sont gardées mais on en parlera plus tard.

Il est donc facile pour les opérateurs (donc les keufs) d'avoir la liste des téléphones ayant servi pour telle carte SIM ou tel numéro de téléphone, ainsi que la liste des cartes SIM ayant été branchées dans tel téléphone.

S'il y a plusieurs emplacements SIM dans un même téléphone, il faut considérer qu'ils sont liés entre eux. Sur internet[8], on peut trouver les différents IMEI d'un même téléphone et parfois aussi la couleur de la coque, la marque, les dimensions, les informations basiques du téléphone, etc. Donc s'il y a 2 cartes SIM dans un même téléphone, les opérateurs peuvent facilement savoir que c'est le même téléphone qui utilise les 2 cartes SIM.

8 Pour voir ces infos, rendez-vous sur ce site : https://www.imei.info/

Sauvegarde

- **Seedvault** (pas hyper simple à utiliser)
- Faire des sauvegardes manuelles…

Podcasts

- **AntennaPod**

Horloge

- **Horloge** Fossify

Sécurité

- **Hypatia Antivirus** pour Android, vous permet de scanner vos documents et votre système afin de détecter la présence de virus connus
- **Extirpater** (effacer l'espace disque disponible) - Écrase la mémoire libre du téléphone (shred) permet de s'assurer que même lorsqu'on supprime des documents sur le tel, il sera difficile pour quelqu'un de les récupérer. Attention pour des documents vraiment sensible, à cause du fonctionnement de la mémoire du téléphone, des données peuvent subsister dans d'autres partis du téléphones.
- **Duress** (réinitialisation du téléphone sur code de déverrouillage spécial)
  ATTENTION: Duress utilise les services d'accessibilité, donc pour les versions antérieures à Android 10, il désactive le chiffrement du téléphone pour fonctionner !
- **Wasted (Permet d'autodétruire votre téléphone en cas de panique.** L'appli va formater et réinitialiser l'OS et, une fois l'opération finie, on aura un téléphone tout propre ⚠ Pour garantir la sécurité de vos données effacées, il faut impérativement que votre téléphone soit chiffré avant de l'autodétruire.) Pensez à gérer vos sauvegardes !
- **AirGuard**, application pour détecter les Airtag, qui sont des petits traqueurs matériels faciles à trouver dans le commerce [défense spécifique].

Séparations des comptes sur smartphone (Profils d'utilisateurs)

La séparation des comptes permet de séparer plus strictement les identités entre différents usages d'un même téléphone. Ça rend compliqué pour une app de chopper les infos d'une autre app installée sur le deuxième compte.

- Sur beaucoup d'Android, et notamment les versions 10 et plus, il est possible d'activer les **"Comptes d'utilisateur"** ou **"Profils d'utilisateurs" ou "Profil professionnel"**, qui permettent d'avoir une séparation plus rigide des apps.
  Quand on utilise un système d'exploitation tel que **GrapheneOS** ou **LineageOS**, on peut activer cette fonctionnalité, installer F-Droid dans tous

- Appels **Signal**
- **Wire** (à 2)

Calendrier/agenda

- **Fossify Calendar** (fonctionne hors-ligne)
- **Etar – OpenSource Calendar**
- **DAVx**[5] (synchronisation de calendrier distant, avec Nextcloud par exemple. Compatible avec **fossify Calendar** ou **Etar**)

Notes

- **Fossify Notes** (hors-ligne, avec un super widget)
- **Nextcloud Notes** (pour synchroniser avec un nextcloud)
- **Standard Notes** : notes chiffrées de bout en bout en local et sur le cloud (dispo en version ordi aussi)

Pare-feu

- **Netguard** (impossible de l'utiliser en même temps qu'un VPN)

Isolation d'applis

- Gestionnaire de **Profils d'utilisateurs** natif du téléphone
- **Shelter**
- **Private Space** : à partir d'Android 15, il est possible de créer un espace isolé depuis les Paramètres du téléphone.

Navigation web

- **IronFox** + installer le plugin **uBlock Origin** pour bloquer les pubs
- **Vanadium** : une version renforcée de chrome pour les personnes qui préfèrent les navigateurs sous chrome. Développée par l'équipe de **GrapheneOS.**
- **Cromite** : un dérivé libre de Chrome intégrant un bloqueur de pubs
- **Tor Browser**

Alternatives à Youtube/Bandcamp/Soundcloud/Framatube

- **NewPipe** (à installer depuis les dépôts de Newpipe en ajoutant le lien du dépôt dans les paramètres de F-Droid) ou **PipePipe** (Très léger mais expose votre adresse IP aux serveurs de Google)
- **LibreTube** (similaire à **NewPipe** mais se connecte à https://piped.kavin.rocks et donc ne contacte jamais directement Google)
- **RiMusic** (équivalent de **Youtube Music**)

Cartes

- **Comaps** (basé sur **OpenStreepMap**, cartographie collaborative en ligne)
- **OsmAnd** (idem)
- **GMaps WV** (isole une page web pour accéder à **GoogleMaps**)

Les opérateurs téléphoniques ont légalement une obligation de supprimer ces informations d'identification au bout d'un an. On n'a pas d'assurance à 100% que cela soit fait, de plus si les infos des opérateurs ont déjà été données à des services de renseignement tels que la DGSI (Direction Générale de la Sécurité Intérieur), c'est probable que cette dernière instance garde les données plus longtemps.

À partir du numéro de téléphone, il peut être possible d'estimer l'opérateur d'une ligne téléphonique, les 4 chiffres après le 06 / 07 étant attribués à ceux-ci[9]. Cependant avec la « portabilité » des numéros ça peut être plus compliqué que cela, car il est possible de changer d'opérateurs en gardant le même numéro.

3179 où comment se faire identifier rapidement à partir de son tel

Si un téléphone appelle le 3179, il reçoit par vocal puis par SMS *a minima* son RIO (Relevé d'Identité d'Opérateur). Il est composé d'une suite de chiffres et lettres donnant ces infos :

1. Les deux premiers chiffres indiquent l'**opérateur concerné** (01 pour Orange et Sosh, 02 pour SFR, 03 pour Bouygues et B&You...)
2. La lettre suivante indique le **type de client** (E pour Entreprise et P pour Particulier)
3. Les 5 caractères suivants indiquent le **numéro de contrat** auprès de l'opérateur
4. Les 3 derniers caractères constituent le **code de contrôle** pour vérifier la correspondance entre le RIO et le numéro de la ligne mobile.

Qui plus est, chez certains opérateurs, il est aussi envoyé le nom et prénom de la personne indiquée à l'opérateur lors de l'enregistrement de la SIM. Dans certains coins, c'est utilisé par des contrôleurs pour vérifier l'identité donnée. Information à avoir en tête lorsque tu leur dis que tu as ton téléphone. Tu peux vérifier en amont sur ton téléphone quelles informations arrivent sur ton téléphone via cette opération. Les opérateurs prépayés type Lyca ne renvoient que le RIO.

Adresse MAC du téléphone

Chaque équipement réseau a une **adresse matérielle unique**. La carte wifi du téléphone a un identifiant qui s'appelle « adresse MAC » qui est fourni à un réseau wifi à sa connexion (et qui est enregistré par le fournisseur d'accès internet pendant 1 an) et est visible localement tant qu'il est activé.

Contrairement au numéro IMEI, il est souvent (pas toujours) possible d'usurper l'adresse MAC, c'est-à-dire en fournir une autre que celle du matériel. L'adresse

9 Vois la liste des préfixes des opérateurs téléphoniques : https://fr.wikipedia.org/wiki/Liste_des_pr%C3%A9fixes_des_op%C3%A9rateurs_de_t%C3%A9l%C3%A9phonie_mobile_en_France

MAC du wifi des smartphones sous Android 10 sont randomisées[10] lors de la recherche de réseau uniquement. À partir d'Android 12, c'est souvent randomisé de tout temps (mais stable, donc l'adresse MAC est unique à chaque réseau et ne sera pas changée en cas de reconnexion au même réseau). Certains fabricants désactivent cette fonctionnalité, donc on ne peut pas s'y fier sans vérification (à part sous GrapheneOS).

Adresse IP du téléphone

À chaque fois qu'on consulte un site internet avec un navigateur sur un téléphone, qu'on utilise l'application d'un réseau social, qu'on communique avec WhatsApp ou Signal, on se connecte à internet. Internet fonctionne avec des adresses IP. L'adresse IP (et même le numéro de téléphone pour les SMS/appels) sont comme l'adresse qu'on met sur une enveloppe postale. Sans ça, notre destinataire ne peut pas recevoir le courrier qu'on lui envoie. Et on ne peut pas recevoir ce qu'on nous envoie.

Quand un appareil est connecté à un réseau wifi, il utilise l'adresse IP de ce wifi (wifi public, box, ou autre téléphone via un partage de connexion). Mais un téléphone possède sa propre adresse IP qui permet de se connecter au réseau internet avec ses données mobiles (en 3G/4G/5G). L'adresse IP d'un téléphone est souvent dynamique, ça veut dire qu'elle évolue dans le temps : une nouvelle peut être attribuée à chaque fois qu'on se connecte. Mais l'opérateur téléphonique en garde une trace même si elle évolue et associe les adresses IP au numéro de téléphone.

L'opérateur – et donc les flics – peut avoir accès à tous les sites qu'on visite, peut déduire les applications de communication utilisées (si elles utilisent un serveur centralisé). Cependant la plupart du temps ils n'auront pas accès au contenu de ce qui est fait sur le site. Cela dépend de :

- Si la connexion est en HTTP, ils voient tout (contenu du site, page spécifique sur laquelle on est, échanges entre notre ordi et le site)

- En HTTPS, ils voient juste le nom du domaine mais ne peuvent pas savoir sur quelle page spécifique on va. Parfois, les sites mélangent du HTTP et du HTTPS.

Si une réquisition est faite par les flics auprès des sites visités, ils peuvent donc remonter à un wifi ou un numéro de téléphone. Pour contrer ça, on peut utiliser un VPN ou Tor (voir dans la suite de la brochure).

Factures téléphoniques détaillées ou fadettes

Il s'agit de toutes les informations autres que le contenu même de la conversation : les fadettes mentionnent les numéros, dates, heures et durées de communication. Les opérateurs gardent les « factures détaillées » (ou FADET / fadettes) pendant 5 ans car c'est une autre législation : c'est de la législation fiscale. Ce temps correspond au délai de contestation possible des factures. Mais le cadre légal ne

10 Il s'agit de l'opération de fournir une adresse mac aléatoire au réseau.

- **Mullvad VPN** – bien en termes de confidentialité et rapidité (payant, 5€/mois pour 5 comptes, possibilité de payer en liquide)
- **CalyxVPN**
- **Orbot** : pour faire passer les connexions des autres applis par **Tor** (ne marche pas pour toutes les applis), ni avec l'utilisation en parallèle d'un pare-feu (firewall) tel que **NetGuard**

Coffre fort à mot de passe

- **KeepassDX** : à partir d'un mot de passe primaire, permet de stocker ses autres mots de passe de manière sécurisée

Autres applis de sécurité

- **Exodus Privacy** : analyse les applications pour lister les pisteurs et les autorisations.

- **Ente Auth** : application pour avoir une double authentification

Photos

- **Open Camera**
- **Obscuracam** : qui peut être configuré pour flouter les visages automatiquement.
- **Scrambled Exif** : pour supprimer les métadonnées d'une image
- **Cryptocam + OpenKeyChain :**chiffrement direct des photos et vidéos avec OpenPGP. Nécessite « Cryptocam Companion /CLI » pour ouvrir les vidéos dans l'ordi. Demande quelques connaissances et un peu de lecture de tutoriels en anglais, sur cryptocam.gitlab.io.

Gestionnaire de fichiers

- **Fossify File Manager** : important de remplacer son gestionnaire de fichier par un gestionnaire de fichier libre, non-connecté à internet et sans pubs !

Vidéos / musique

- **VLC**

Lecture de documents

- **Secure PDF Viewer** (par défaut sur GrapheneOS) : nécessite la dernière version d'Android, vraiment sécurisé.
- **Librera** (pour lire des ebooks)
- **MuPDF** (pour afficher PDF et autres)

(i) *Bonus : plein d'ebooks à télécharger sur trantor.is, z-lib.org, libgen.rs*

Audio/visio-conférence

- **Jitsi** (audio/vidéo à plusieurs) (meet.systemli.org ; vc.autistici.org)
- **Plumble** (protocole Mumble, audio uniquement)

Lorsqu'il y a à la fois Aurora store et le Google Play Store, les mises à jour des applis peuvent être faites par défaut par le Play store, même si elles sont installées par Aurora store. Ça vaut le coup de désactiver le Play store si Aurora store a été installé.

- **Obtainium** : permet d'installer et mettre à jour des applis directement depuis leurs dépôts GitHub / GitLab / F-Droid ou d'autres serveurs sans liens avec Google. C'est bien pour des utilisateur·rices d'Android déjà à l'aise avec le bidouillage de téléphone.

Messageries instantanées visant à protéger la confidentialité des communications

- **Signal** (ou **Molly** qui ouvre plus de fonctionnalités de sécurité) : permet de communiquer de manière chiffrée mais le compte est relié à un numéro de téléphone (voir nos recommandations de paramètres dans la suite de la brochure).
- **Briar** : protocole de chiffrement Briar, compte pas relié à un téléphone, utilise Tor si on veut, fonctionne aussi sans internet (via Bluetooth).
- **Conversations** : protocole de chiffrement XMPP/Jabber
- **Element** : protocole de chiffrement Matrix.
- Cwtch (https://cwtch.im/)

Applis visant à protéger l'identité de leurs utilisateur·ices

- **Tor Browser** (pour naviguer sur le web anonymement)
- **Orbot** (pour faire passer toutes les communications du téléphone sur le réseau **Tor**)
- **Briar** (pour échanger des messages instantanés chiffrés sans donner de numéro de tel ou d'e-mail)
- **Conversations** (pour échanger des messages instantanés chiffrés)

Pour les SMS

- **QUIK SMS** (anciennement **QKSMS**)
- Fossify **SMS Messenger**
- l'appli de SMS de base d'Android Open-Source Project

Pour les e-mails

- **Thunderbird mail** (remplace K-9 Mail)
- **FairEmail**

(i) Ces deux clients* permettent d'accéder à vos e-mails depuis votre téléphone, mais aussi de de chiffrer ses e-mails avec PGP à l'aide de OpenKeyChain.

VPN

- Versions gratuites : **RiseupVPN** (prix libre), **Proton VPN** (freemium)

permet en théorie pas aux flics d'en demander l'accès au-delà **d'un an**. Cependant dans le cadre d'une enquête passée, certaines données peuvent être mises dans un dossier et dans ce cas être utilisées plus tard.

30 000 flics ont accès depuis juin 2022 au logiciel *DeveryAnalytics Telephony Data* qui permet d'aider à l'analyse de fadettes et autres données de masse[11].

Des nouvelles jurisprudences de la cour de cassation du 12 juillet 2022 peuvent permettre de contester dans certains cadres l'utilisation dans les procès de preuves obtenues à partir de fadettes.[12]

Failles de sécurité et mises à jour 📱

Une faille, c'est une erreur, un défaut ou une vulnérabilité dans un système informatique. Ça peut apparaître dans chaque logiciel, de l'application de chat qu'on utilise quotidiennement au système d'exploitation du téléphone, en passant aussi par le pilote matériel qui permet de faire fonctionner le port USB ou la prise jack.

Aucun logiciel n'est parfait, tant qu'il y aura des logiciels, il y aura des failles de sécurité. L'existence de failles ne veut pas dire que des personnes les exploitent, mais il faut garder à l'esprit que de tout temps les logiciels ont été attaqués, et le seront encore. Même les meilleurs logiciels de sécurité, même quand c'est les meilleurs ingénieur·e·s du monde qui ont bossé dessus.

Quelques exemples de failles de sécurité découvertes ces dernières années :

En 2015 : sur Android, on pouvait recevoir un MMS trafiqué qui donnait accès aux audios et vidéos et la carte SD du téléphone.

En 2019 : sur iOS, 4 failles de sécurité permettaient de prendre le contrôle d'un téléphone en amenant l'usager·e à se connecter à un site internet malveillant ; sur Android, il était possible de déclencher une réponse à un appel Signal[13].

En 2020 : sur Android 8 et 9 et la plupart des Linux, avec le bluetooth allumé mais non-connecté, un·e attaquant·e pouvait prendre le contrôle et aspirer toutes les données. Cette faille a été corrigée, mais bon nombre de téléphones n'ont juste jamais de mises à jour et sont donc toujours vulnérables… Pour s'en protéger il faut couper le bluetooth.

Comme déjà dit, des failles de sécurité seront toujours découvertes. Parfois corrigées avant d'être rendues publiques, parfois utilisées par des adversaires pendant plusieurs années avant d'être corrigées. C'est pourquoi il est extrêmement important d'**appliquer les mises-à-jour au maximum**, que ce soit sur nos ordis ou

11 Le site internet du producteur de logiciel: https://www.chapsvision-cybergov.fr/deveryanalytics/

12 https://www.courdecassation.fr/toutes-les-actualites/2022/07/12/enquetes-penales-conservation-et-acces-aux-donnees-de-connexion

13 Source: https://www.cvedetails.com/cve/CVE-2019-17191/

nos téléphones. Il est important que les applications et le système d'exploitation qu'on utilise soient suivies dans le temps, que l'équipe de développement corrige les failles de sécurité découvertes. En termes de confiance, on peut se renseigner sur la réactivité et les développeur·euses lorsqu'une faille est connue et la communication qu'iels en font. Ça peut être déterminant sur le choix du système d'exploitation ou des applications qu'on installe.

On peut savoir combien de temps sont suivis pas mal de modèles de téléphones sur ce site : https://endoflife.date

Données de la carte SIM et du téléphone [ ]

En cas d'accès physique à la carte SIM et au téléphone :

- Activer préalablement le code PIN de la carte SIM peut rendre plus compliqué à des flics de base l'accès à certaines informations. Cependant, ce code PIN est aisément contournable grâce au code PUK que les flics peuvent demander aux opérateurs (pour la modique somme de 3 euros) ou grâce à des outils d'extraction. Il n'est pas possible de protéger de manière sûre les données stockées dans une carte SIM (IMSI, contacts, etc.).

- Les données d'un téléphone non-chiffré* et les données de nombreux modèles de téléphone même chiffrés sont accessibles par des outils que nous verrons dans le chapitre suivant.

Communiquer c'est à plusieurs [ ]

La communication c'est par définition un truc qui se fait à plusieurs. Les outils et pratiques qu'on choisit d'utiliser de son côté ne sont pas forcément les mêmes chez les autres. Si j'ai le téléphone le plus sécurisé du monde, mais que des potes m'appellent en clair pour me demander si je vais à telle réunion ce soir, leurs pratiques peuvent rendre les miennes caduques.

- Ne pas se sentir infaillible parce qu'on chiffre son tél ou qu'on a des bonnes pratiques de son côté.
- Les pratiques collectives sont à discuter ensemble et il est important de se soutenir dans la mise en place d'outils.
- Dans la suite, il y a un certain nombre de conseils d'autodéfense numérique. Cela permet notamment d'assimiler petit à petit la théorie et l'usage de chaque pratique, permettant à la fois une meilleure maîtrise sur le long terme et une transmission collective plus facile.

• nombre d'utilisateur·rices : est-ce qu'une poignée de gens utilisent le logiciel ou pleins de gens, dont des « expert·es » qui peuvent faire un audit ?
• modèle économique du logiciel : est-ce qu'on vend mes données, est-ce qu'il y a des services payants, est-ce que c'est financé par des dons ?
• libre : est-ce un logiciel privatif, open-source, libre (voir ci-dessous) ?
• coût financier et technique : est-ce que l'utilisation de l'outil demande beaucoup de ressources ou non ? est-ce qu'il demande beaucoup de connaissances techniques ?
• public « cible » : cet outil s'adresse-t-il à tout le monde ? aux militant·es ? aux gens qui ont de l'argent ?
• l'enjeu des phénomènes de mode : est-ce qu'on utilise ce logiciel parce que tout le monde l'utilise ou parce qu'elle a vraiment une bonne réputation ?

Une tendance lorsqu'on parle de sécurité est d'utiliser des logiciels libres*. Pourquoi ?
• Avec une appli privative, on ne pourra pas vérifier profondément la qualité de l'appli en termes de sécurité ; et les développeur·ses peuvent décider d'arrêter le développement de l'appli sans préavis. Une appli libre* permettra à une communauté de scruter son fonctionnement et, avec un peu de chance, de reprendre le développement si l'équipe d'origine abandonne le projet (exemples : navigateur Mull repris pour faire IronFox).
• Une appli non-libre* pourrait volontairement chercher à nuire (de manière large ou de manière ciblée), sans qu'on puisse s'en apercevoir sans l'installer, car sa recette n'est pas rendue publique. Exemples : Skype, malwares et ransomwares cachés dans des jeux, etc.

⚠ Attention, **libre ≠ sécure**. Une appli libre* peut contenir du code malveillant (volontairement ou non).
Enfin, il est important de bien **toujours mettre à jour ses applis**, afin de profiter des correctifs de sécurité.

Voyons quelques applications, pas toutes fiables pareillement, pas toutes mises à jour régulièrement, mais toutes libres*.

Magasin d'applications

- **F-Droid** : propose des applis principalement libres. Attention tout ce qui est dans F-Droid n'est pas forcément extraordinaire : il peut y avoir des pisteurs dans les applications (mais dans ce cas-là, on peut le savoir), des bouts d'applis qui ne sont pas libres ou encore des failles de sécurité connues, etc. Une partie de ces applis contre-indiquées sont recensés sur le site de F-droid dans leur liste "d'antifonctions": https://f-droid.org/fr/docs/Anti-Features/
- **Aurora Store** (interface libre au **Google Play Store**, permettant de l'utiliser sans compte Google) (rappel : les applis dans le Play Store sont pour la plupart non-libres et peuvent potentiellement être modifiées par Google).

→ Quelle énergie avons-nous à mettre pour nous protéger ?

Quelques habitudes à mettre en place si ça nous paraît cohérent :
• Se demander à chaque fois comment faire sans téléphone, si possible, par exemple en laissant son téléphone chez soi ou chez un·e ami·e
• Il est plus difficile d'accéder aux données d'un téléphone chiffré quand il est éteint plutôt qu'allumé. L'éteindre / le laisser éteint s'il y a des risques de perquisition / d'interception. Mettre un mot de passe conséquent, 6 mots aléatoires si on n'utilise pas **GrapheneOS**.
• Rendre habituels certains usages, comme le mode avion par exemple.
• Stocker le moins de choses possible sur le téléphone (documents, photos, contacts, messages). Penser à transférer les photos et fichiers, les téléverser dans un ordi de confiance, ou sur un support USB chiffré*.
• Avoir des téléphones différents pour des usages différents. Avoir un téléphone professionnel, un téléphone militant qu'on peut décider de ne pas allumer chez soi. C'est parfois complexe à appliquer mais intéressant pour compartimenter ses activités. Il est aussi possible que ça soit pris en charge collectivement : que le collectif fournisse des téléphones anonymes pour une tache spécifique dans la lutte.
• La NSA a dit « redémarre ton tel une fois par semaine ». S'il y a une faille exploitée mais pas inscrite dans le téléphone, en redémarrant les éventuels logiciels malveillants présents dans la mémoire vive ne seront plus là.
• Faire de la veille politique et technologique, se former soi-même ou avoir un collectif qui se forme. Les téléphones évoluent très rapidement !
• Se former collectivement en cas de garde à vue : BD « je n'ai rien à déclarer » sur infokiosques.net, ou « manuel de survie en garde à vue », livre « comment la police interroge et comment s'en défendre » sur projet-evasions.org.
• Ne pas avoir de téléphone :)

2) Applications libres 📱

⚠ Attention ces informations datent de l'été 2025
et peuvent évoluer particulièrement vite !

Comme on l'a vu, les applications ont un grand pouvoir de surveillance. C'est pourquoi on peut choisir d'utiliser des applications « de confiance ». Mais alors il faut définir ce que « confiance » signifie, et comment acquérir cette confiance.

La **confiance** en une appli peut se jouer à différents endroits. Voici une liste non-exhaustive de critères à prendre en compte :
• sécurité : l'appli fait-elle bien ce qu'elle dit et dit-elle bien ce qu'elle fait ?
• fiabilité dans le temps : est-ce que les gens continuent de travailler dessus pour corriger les vulnérabilités ou d'améliorer le service ?
• réputation des développeur·ses qui font le logiciel : sont-ils réactif·ves quand il faut corriger des failles découvertes ?

III) Outils des keufs

Par les dossiers pénaux ou des révélations d'informations, on a des éléments de pratiques utilisées dans des dossiers judiciaires pour tout ce qui touche au domaine policier, mais il est compliqué de connaître les pratiques réelles des services de renseignement[14].

Interceptions administratives et judiciaires [ ]

La police peut faire des réquisitions auprès des opérateurs, soit pendant une enquête ou un évènement spécifique, soit après coup. Une panoplie de choix est à leur disposition[15], ça peut s'appliquer :

- sur une antenne en particulier : identifiants IMEI et/ou IMSI, modèle des téléphones, opérateurs téléphoniques des lignes ayant borné à telle antenne à tel moment.
- sur un téléphone ou un carte SIM spécifique : données fournies à l'opérateur – comme l'adresse mail, les coordonnées bancaires ou l'identité, historique des cartes SIM mises dans tel téléphone, liste des téléphones ayant servis à telle carte SIM, modèle du téléphone utilisé, factures détaillées (voir dans la partie correspondante), code PUK (permet de déverrouiller le code PIN de la carte SIM), mise sous écoute en temps réel (cela renvoie en parallèle l'appel sur le téléphone d'un flic), la géolocalisation en temps réel, les sites consultés (pas toujours possible, et quand la connexion est en https ça ne concerne que les noms de domaines visités, pas les pages exactes), etc.
- pour faire de l'identification en masse : demander l'identité associée à plusieurs centaines de numéros de téléphones d'un coup. Les délais de réponse sont de l'ordre de l'heure.
- faire une recherche auprès de chacun des opérateurs pour obtenir le numéro de téléphone à partir de l'identité d'une personne. Ça nécessite pour les flics de vérifier les numéros récupérés par cette méthode (homonymes, faux noms…) ça n'est pas pratique d'usage pour eux.

Une plateforme a été créé pour automatiser, conventionner les tarifs et fluidifier le travail avec les opérateurs : la PNIJ, pour plateforme nationale des interceptions

14 Il est possible de fouiller dans les rapports de a CNTCR - Commission nationale de contrôle des techniques de renseignement pour avoir les infos qu'ils veulent bien nous fournir : https://www.cnctr.fr/8_relations.html. Par exemple on y apprend en ordre de grandeur que 5 000 personnes sont sous écoute des renseignements chaque année.

15 On peut s'intéresser à fouiller parmi les différentes possibilités offertes aux flics, avec les prix de chaque opération sur legifrance (Tarifs hors taxes applicables aux prestations requises aux opérateurs de téléphonie mobile) : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000041553495

judiciaires (résultat d'un partenariat public-privé avec Thales)[16]. Légalement, la demande des flics doit passer par cette plateforme, dans la pratique et aussi parce que la PNIJ n'a pas de contrat avec tous les opérateurs (notamment les opérateurs non français), 25 % des demandes ne passent pas par la PNIJ[17].

Données faciles à obtenir à distance par la police

- Données d'identification
- Identifiant carte SIM
- Factures détaillés
- Mise sous écoute (plus coûteuse en terme financier, moins fréquent)

Géolocalisation via les évènements réseaux

L'antenne de connexion enregistre un certain nombre d'information : le passage d'une antenne à une autre, si le téléphone s'éteint, s'allume ou se met en mode avion. Ces éléments s'appellent évènement réseau et, s'ils sont demandé, ils permettent d'avoir une géolocalisation approximative du téléphone lorsqu'il est allumé. Approximative car c'est juste une antenne qui enregistre la donnée, il faut une réquisition de géolocalisation en temps réelle pour avoir une géolocalisation précise. La géolocalisation précise ne peut pas se faire après coup, elle doit être demandée sur une période de temps donnée.[18]
Ces évènements réseaux peuvent être demandés par réquisition sur un téléphone, ou sur une antenne précise. Ces données ne sont pas présents dans les fadettes et sont censées êtres conservées 1 an. D'après la brochure « affaire lafarge, les moyens d'enquête utilisés et quelques attentions à en tirer » Free n'enregistrerait pas (ou ne communiquerait pas) ces évènements réseaux à la demande effectuée dans le cadre de cette enquête.
Il y a une localisation associée à chaque communication du téléphone (toute réception ou émission de sms, appel ou data paquet, c'est-à-dire toutes connexions téléphone à internet), car il est enregistré le nom et la localisation de l'antenne la plus proche du téléphone. Cette géolocalisation est plus fréquemment demandée par la police que les évènements réseaux.

16 Dans un commentaire du ministre de la justice fin 2018 qui donne l'ampleur de la plateforme : « La PNIJ est ainsi aujourd'hui, pleinement opérationnelle et utilisée par plus de 60 000 magistrats, enquêteurs et greffiers. Elle traite plus de 11 000 interceptions simultanées et 6 000 demandes de prestations annexes par jour. Elle intercepte près de 800 000 communications et 1,2 million de SMS par semaine. » https://questions.assemblee-nationale.fr/q15/15-13319QE.htm

17 Rapport du sénat du 15 novembre 2023, « Surveiller pour punir ? Pour une réforme de l'accès aux données de connexion dans l'enquête pénale »

18 Voir la vidéo de Christophe Bounty, comment la police géolocalise votre téléphone

IV) Mesures d'atténuation de la répression

⚠ Attention ce chapitre évolue particulièrement vite dans le temps. Se renseigner sur l'évolution au cours du temps.

Vous pouvez retrouver cette partie sur le wiki https://telmob.0id.org/. Il s'agit d'un wiki donc il est possible de contribuer / modifier.

La sécurité absolue pour les téléphones est impossible. Ce que l'on veut, c'est développer des mesures d'atténuation de vols et fuitages de données que nos adversaires peuvent utiliser contre nous.

Pour réduire les risques, avoir plus de contrôle de ses communications, plusieurs outils sont à notre disposition.

On peut classer ces outils en quelques catégories :

- habitudes, manières d'utiliser le téléphone, questionner les usages

- choix d'applications

- paramètres du téléphone

- avoir un téléphone « anonyme »

- les trucs avancés en terme technique

1) Habitudes [✆]

Le plan des habitudes est le plus important, car comme on l'a vu, utiliser des téléphones portables implique un grand nombre de problèmes inévitables.

* La première habitude à prendre consiste à se poser les bonnes questions. La « modélisation de la menace » est un outil nous permettant de choisir des réponses adaptées à nos besoins. C'est un outil à expérimenter et utiliser individuellement et collectivement car nos choix auront des conséquences sur notre entourage.
→ Qui sont nos ennemi·e·s potentiel·les ? (flics en garde à vue, agent de renseignement derrière son ordi, agent en filature, fachos, voisin·nes, cohabitant·es, patrons…)
→ Que veut-on leur cacher ? (liste de contacts, membres d'un groupe Signal, contenu de message, localisation, sites web visités, documents enregistrés…)
→ Que risquons-nous si on échoue ? (se faire gronder, perdre nos données, prendre une amende, aller en prison…)
→ Quels moyens nos ennemi·es sont-iels prêt·es à mettre pour nous ou nos activités ? (respect de la loi ou pas, quantité d'argent disponible, protection légale…)

À savoir qu'en plus des prix des logiciels, il y a des enjeux géopolitiques autour des logiciels utilisés ce qui peut expliquer le fait qu'ils ne sont pas utilisés partout. En fonction de quelle entreprise ou pays propose le système de surveillance, les utiliser dans le renseignement français, c'est donner des accès à ce qui intéresse les renseignements à ces structures.

En garde à vue / audience / instruction / enquête 📱

Lors d'une garde à vue, notre droit au silence est limité, entre autres, par l'« obligation de fournir la convention secrète de déchiffrement ». Cette obligation s'applique notamment aux téléphones, si la demande est faite dans son cadre. Dans ce cas, refuser de donner les mots de passe peut amener en soi un risque de procès. Le cadre permettant qu'une telle demande nous soit faite est le suivant :

- la demande doit être fait par un OPJ (Officier de Police Judiciaire, pas un flic « de base ») supervisé d'un magistrat – procureur ou juge d'instruction.
- elle doit être justifiée, il doit être démontré que le téléphone utilise des méthodes de cryptologie, et que le déverrouillage pourrait permettre d'accéder à des éléments pertinents pour avancer dans l'enquête en cours (« l'enquête ou l'instruction doivent avoir permis d'identifier l'existence des données traitées par le moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit »). S'il ne semble pas y avoir d'enquête approfondie, il ne devrait pas être possible d'y avoir condamnation pour cela.
- il faut qu'il soit démontré que tu connaisses ce code de déverrouillage.

Tout cela doit être explicitement formulé pour que ça soit accepté dans un cadre légal. Si l'évolution judiciaire ne va pas dans le bon sens au cours du temps, **il reste toujours conseillé d'appliquer les mêmes règles qu'habituellement en garde à vue « je n'ai rien à déclarer » en cas de demande de code de déverrouillage** (et pas « je sais pas » ou autre)[19]. Ces poursuites ne semblent pas fréquentes, et c'est souvent utilisé comme chef d'inculpation qui en complète d'autres. L'avantage d'exercer ton droit au silence c'est que tu pourras choisir ta défense en cas de poursuite, bien des possibilités peuvent exister.

Le Kiosk – extracteur du contenu d'un téléphone 📱

Fabriqué par l'entreprise israélienne « Cellebrite » (qui, en pleine participation active aux génocide palestinien en juin 2025, affirme cyniquement sur son site en bandeau central « Nous avons pour mission de

19 Voir l'article de mai 2021 « Du nouveau sur l'obligation de donner son code de téléphone en garde-à-vue : comment éviter le traquenard » https://paris-luttes.info/du-nouveau-sur-l-obligation-de-15018 trouvable en format brochure sur https://rajcollective.noblogs.org/materiaux-a-diffuser/

mettre fin aux crimes contre les enfants »), le Kiosk est vendu à des acteurs étatiques. C'est une version tout-compris de leur outil « UFED » (Appareil d'extraction forensique universelle). 500 Kiosks ont été achetés en France pour les flics, à 8000 euros l'unité, installés « d'ici 2023 » (d'après des sources de 2020). C'est un ordi tactile, avec des gros boutons et plein de câbles : il va essayer d'aspirer le contenu du téléphone et de générer des rapports valables aux yeux des magistrats (analyse forensique = sans dégradation du matériel). Il y a régulièrement des articles publiés, contenant des listes de téléphones qu'ils arrivent à craquer, des listes d'applis prises en charge par l'extraction de données[20].

Pour fonctionner, l'UFED exploite des failles de sécurité présentes dans la partie du système d'exploitation qui gère le port USB. Ces failles de sécurité peuvent être déjà publiques ou découvertes par les ingénieurs de Cellebrite. D'autres peuvent être achetées sur internet pour des sommes allant quelques dizaines de milliers à plusieurs millions d'euros, ce qui n'est pas grand chose pour ce genre d'entreprise.

L'UFED peut contourner très facilement les codes de déverrouillage des téléphones non-chiffrés* ou des téléphones chiffrés* mais allumés et cloner la carte SIM.

Pour les téléphones chiffrés et éteints, UFED peut aussi permettre un déchiffrement d'un grand nombre de téléphones. En effet, dans le cadre d'enquête approfondie (probablement via le Centre Technique d'Assisance de la police), l'UFED peut être utilisé sur une très large gamme de téléphone, la plupart des Android non-Pixel (et non antérieurs au Pixel 6a), ainsi que les modèles antérieurs à iOS 12, peuvent subir des attaques « bruteforce » sur le mot de passe, et donc, lorsque le mot de passe est simple, souvent permettre de récupérer le contenu complet du téléphone rapidement.

20 En avril 2025: https://osservatorionessuno.org/blog/2025/03/a-deep-dive-into-cellebrite-android-support-as-of-february-2025/, « A deep dive into Cellebrite: Android support as of February 2025. »

Outil d'analyse des flics qui leur permet de faire des graphes de qui parle avec qui, ils injectent dans le logiciel toutes les informations récoltées principalement dans les communications téléphoniques (que ce soit sur les personnes, lieux, évènements, le matériel). Ainsi, dans les enquêtes sur des militant-es, ils essayent de mettre en avant des « organisateur·ices » de tel mouvement qui est en contact avec beaucoup de personnes militantes, ou des personnes qui font liens entre plusieurs univers.

Tentative de restauration des données à partir d'appareils endommagés [⤷]

On n'a pas d'éléments d'usage à ce sujet, mais il existe des corps de police qui essayent de récupérer des données de supports numériques cassés ou partiellement brûlés[24]. Ces techniques semblent être utilisées dans des affaires plus importantes.

Installation de mouchards (matériel ou logiciel) [⤷]

Cela semble plus être pratiqué dans un cadre de renseignement que dans des cadres utilisables judiciairement. Par exemple, l'installation d'un mouchard qui surveille ce qui se passe sur les autres applications, allumer les micros à distance, activer et transmettre la géolocalisation, feindre que le téléphone est éteint. Les mouchards peuvent être matériels, ce qui nécessite d'avoir accès à l'appareil, ou logiciels en installant à distance ou à partir de l'appareil des logiciels malveillants.

Un des logiciels-espions très médiatisé faisant cela est **Pegasus**. Il permet de fouiller dans les données (calendriers, photos, contacts, messageries, appels enregistrés, coordonnées GPS…) des smartphones, iPhones comme Androids, infectés, mais aussi de contrôler à distance la caméra et le micro intégrés à l'appareil, ce qui donne entre autres la possibilité d'écouter des conversations dans une pièce alors que le téléphone apparaît inactif. Un outil avait été développé en 2021 pour essayer de détecter sa présence dans son téléphone mais nécessite des compétences informatiques avancées[25]. En 2021, Pegasus pouvait être installé sur un téléphone en faisant cliquer sur un lien, ou via une faille de sécurité de WhatsApp, la victime recevait ce qui ressemble à un appel vidéo qui suffit à infecter le téléphone dès la première sonnerie, même si elle ne répond pas. À priori, la france n'utilise pas ce logiciel dont le coup d'acquisition pour une structure est à quelques dizaines de millions d'euros.

Voici quelques noms généraux de logiciels malveillants si on a envie de voir leur capacité : PlainGnome, BoneSpy, Monokle, NoviSpy, Mandrake, AwSpy… Ils ne sont pas forcément utilisés par les renseignements français.

24 https://www.nextinpact.com/article/29762/108071-la-nouvelle-arme-anti-cryptographie-gendarmerie

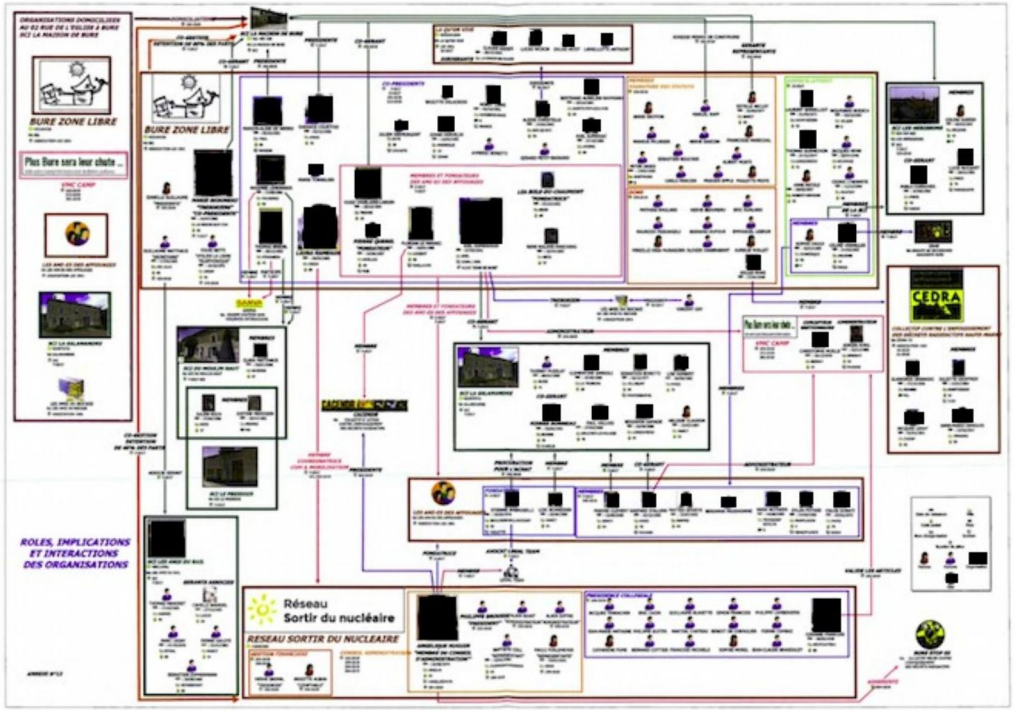
25 Mobile Verification Toolkit : https://github.com/mvt-project/mvt

Plus d'informations sur les équipes techniques:

- "Blog d'un informaticien ancien expert judiciaire" : https://zythom.fr/

- "The french intelligence", compilation de textes sur les renseignements français: https://infokiosques.net/spip.php?article1821

Analyst's Notebook et logiciels d'analyse de données [↘]



Exemple de graphe fait par le logiciel Analyst's Notebook sur une enquête à Bure.[23] *Ce graphe, basé sur les communications entre les gens, permet de ranger chaque personne dans des rôles supposés vis à vis de la lutte.*

Logiciel proposé par I2, filiale d'IBM, le géant des microprocesseurs. Il est utilisé par le Service central de renseignement criminel sous le nom ANACRIM pour analyste criminel (dont on confond souvent le nom de l'équipe d'« Analyse Criminelle » des keufs avec celui du logiciel).

23 Information disponible sur l'article https://reporterre.net/La-justice-a-massivement-surveille-les-militants-antinucleaires-de-Bure qui développe les outils de surveillance utilisés dans le cadre de l'instruction pour association de malfaiteur à Bure, dont beaucoup sur la téléphonie.

Le tableau ci-après montre des exemples d'informations susceptibles d'être collectées dans différents matériels de téléphonie :

Téléphone portable	Smartphone (iPhone, Android…)	Tablette (iPad, Android…)
- Liste de contacts - Messages GSM (SMS) - Journal d'appels - Calendrier - Notes personnelles - Photographies …	- Liste de contacts - Messages GSM (SMS-MMS) - Messageries Internet (WhatsApp, Skype, Facebook Messenger, Telegram, SnapChat, Signal…). - Journal d'appels - Photographies - Vidéos - Géolocalisation - Traces de navigation Internet - Agendas - Notes personnelles - Documents - Messagerie électronique …	- Liste de contacts - Messageries Internet (WhatsApp, Skype, Messenger, Telegram, SnapChat…). - Photographies - Vidéos - Géolocalisation - Traces de navigation Internet - Documents - Agendas - Notes personnelles - Messagerie électronique …

IMSI-catcher – les fausses antennes relais [↘]

Il s'agit d'un dispositif **se faisant passer pour une antenne relai officielle, qui capte toutes les connexions téléphoniques dans un rayon défini**. Il peut être embarqué dans un véhicule, voire dans un sac à dos. Sa première fonction est de lister les appareils téléphoniques alentours. Il peut aussi intercepter les contenus en clair* tels que les appels et les SMS (en forçant le basculement de la communication du téléphone sur de la 2G), mais **il sert principalement à récupérer les métadonnées*** : quel téléphone « borne » (est présent dans le rayon défini), quel téléphone communique avec quel autre téléphone à quel moment, etc.

La police récupère les numéros IMSI et IMEI et peuvent faire des réquisitions auprès des opérateurs pour savoir à qui ça appartient. Un IMSI-catcher ne permet pas de prendre le contrôle d'un téléphone ni d'en extraire les données à distance. Le prix d'un IMSI-catcher de qualité pro est d'environ 2000 euros. Pour 50 euros on pourrait s'en fabriquer un, il aura un faible rayon d'efficacité et on devra trouver les outils permettant de déchiffrer les communications, mais on pourra facilement voir les IMEI alentours et autres infos. Il est aussi possible d'installer un IMSI catcher sur un drone[21].

21 Exemple sur ce site : https://innovadrone.com/drone-imsi-catcher/

Perquisition à domicile [ ]

Il y a plusieurs cadres juridiques à une perquisition, donc quand ça arrive ça peut valoir le coup de demander dans quel cadre on est (enquête préliminaire, flagrance, instruction). Si c'est une enquête préliminaire, on peut parfois refuser la perquisition, ce que les flics ne vont pas préciser. Nous n'allons pas approfondir cette partie, mais il existe un guide appelé « Se préparer aux perquisitions » disponible ici : https://rajcollective.noblogs.org/materiaux-a-diffuser/. Ce qui n'a pas été mis à jour dans ce guide, c'est que depuis quelques années il est possible d'avoir la présence d'un·e avocat·e lors d'une perquisition (cependant le temps qu'iel arrive ne suspend pas la perquisition).

Boites noires

Les boites noires sont des équipements de surveillance algorithmique qui se développent progressivement et servent aux renseignements (Direction Générale de la Sécurité Intérieure). Ces algorithmes se développent aussi bien pour la téléphonie que pour le numérique. Elles font de la surveillance de masse de la population et émettent des signalements, ainsi en 2020 elles ont effectué 1739 alertes de personnes à « comportement suspect »[22].

Globalement elles servent à choper la liste des sites internets qu'on visite. Les boites noires font du traitement automatisé de données. Leur réel fonctionnement reste flou, mais elles ne peuvent pas savoir précisément quelles pages on visite lorsque le site est en HTTPS (avec le S[écurisé] à la fin = la plupart des sites internets). Couplé à d'autres méthodes de surveillance, ça peut permettre de faire des graphes de profilage.

Équipes technologiques de la police [ ]

Tout au long de ce texte, on parle de flics ou de keufs, mais en réalité il existe beaucoup de corps différents au sein de la police, de la gendarmerie et de la justice, qui ont des moyens différents en termes techniques.

La plupart des corps techniques doivent extraire les infos du téléphone sans dégrader celui-ci ni laisser de trace de l'intrusion dans le téléphone, c'est ce qu'on appelle « l'analyse forensique ».

Type de parcours possible lors d'une enquête : il existe une cellule qui travaille sur une instruction, celle-ci envoie au département informatique-électronique l'IRCGN (Institut de Recherche Criminelle de la Gendarmerie Nationale) qui a pour mission d'extraire le contenu d'un téléphone et de le ranger dans un disque dur. Celui-ci peut aussi se déplacer et être présent lors de perquisitions. Si cette institution est

22 https://www.nextinpact.com/article/69817/6-000-comptes-informatiques-sont-connectes-aux-grandes-oreilles-renseignement

bloquée par un support chiffré elle peut décider de l'envoyer au CTA (Centre Technique d'Assistance). Si des informations sont extraites elles sont renvoyées à la cellule d'enquête.

- L'**Institut de Recherche Criminelle de la Gendarmerie Nationale** qui a un statut militaire au sein duquel se trouve le Département informatique-électronique (INL). « *Ce dernier traite de la preuve numérique sur tous types de supports, en particulier sur les disques durs et les téléphones portables. Assurant des expertises judiciaires et des examens scientifiques au profit des magistrats et des enquêteurs, il est également en mesure de les assister sur le terrain ou à distance, lors de perquisitions ou d'auditions en milieu complexe.* » Il dispose d'enquêteur en technologies numériques (N-Tech), qui sont gendarmes, avec une formation d'officiers de police ainsi qu'une formation dans le domaine informatique de 15 mois à l'UTT de Troyes.

- **Le Centre Technique d'Assistance** : « *[...] l'Etat s'est doté dès 2001 d'un organisme à vocation interministérielle, le Centre Technique d'Assistance (CTA) rattaché au ministère de l'Intérieur et aujourd'hui placé sous l'autorité de la DGSI. Il est au service des magistrats et des enquêteurs qui le sollicitent et constitue un niveau d'intervention technique supérieur mis à leur disposition pour augmenter les chances de succès de leurs investigations lorsque les délinquants et criminels ont fait usage de moyens de chiffrement* ». Le CTA est couvert par le secret défense et a le droit d'utiliser des techniques pouvant détruire le matériel à étudier.

L'IRCGN peut être remplacé par des entreprises d'ingénieur·es agrées sous-traitantes comme par exemple :

- Tracip : https://www.tracip.fr/
- Informatique légale : https://informatique-legale.com/
- Laboratoire évidences SAS : https://evidences-lab.com/