Comment éviter que son téléphone ne serve la répression de tou·tes

Cette brochure rédigée fin mai 2024 est une synthèse d'un atelier de discussion collective autour des bonnes pratiques anti-répression liées au téléphone portable. Elle réunie des informations factuelles et des conseils pour éviter de s'incriminer soi, d'incriminer ses camarades, de fournir aux "Forces De l'Ordre"[1] (FDO) des leviers de pression psychologique ou même de faciliter le travail de répression à l'encontre de parfait·es inconnu·es à cause de son téléphone portable. Concrètement, ce texte liste des "menaces", c'est à dire des moyens qu'ont les FDO pour nous réprimer à l'aide de nos téléphones, en fonction de leur probabilité. Ce n'est probablement pas la peine de se blinder contre toutes ces menaces tout le temps et nos stratégies de défense peuvent être adaptées à nos pratiques militantes. Ceci étant, ce n'est pas parce qu'on n'a "rien à se reprocher" qu'il ne faut rien cacher car nos données anodines sont la matière première de la surveillance généralisée et automatisée mise en place progressivement par les FDO pour réprimer d'autres personnes (par exemple à travers la constitution de "graphes sociaux", voir note complémentaires I à la fin).

1 Terme à entendre au sens de tous nos adversaires qui luttent pour le maintien de l'ordre établi (flics ou gendarmes, services de rens, sécurité privées, administrations publiques, fafs...)

Sommaire

A - Premier cas de figure : les FDO accèdent physiquement à ton téléphone

1. Consultation et copie de tes données à un instant T

Probabilité de cette menace : 5/5

En cas de garde-à-vue, de perquisition ou de contrôle en rue, les FDO peuvent légalement prendre ton téléphone et regarder ce qu'ils veulent dedans. Les témoignages convergent qu'ils le font presque systématiquement.

Pour avoir un téléphone qui contient le moins d'informations possibles utilisables par les FDO[2] (à part ce qu'iels peuvent déjà avoir par les fadettes, voir cas B), il est possible par exemple de prévoir un téléphone dédié pour les manif'actions avec risque de placement en garde-à-vue ou de remettre à zéro son téléphone avant chaque manif (ou bien sûr de ne presque jamais se servir du téléphone du tout). Mais il contiendrait quand même quelques informations et cela ne protège de toute manière pas d'une saisie imprévue (par exemple lors d'un contrôle routier).

Pour éviter que les FDO n'aient un accès direct à l'ensemble des données contenues dans le téléphone en cas de saisie, il est possible de chiffrer en amont son téléphone (ou d'avoir vérifié qu'il est chiffré automatiquement) à l'aide d'un mot de passe qu'il faut retenir.

Dans ce cas, on peut prévoir que les FDO peuvent se livrer à deux attaques en parallèle qui sont indépendantes l'une de l'autre :

- **Refus, déni plausible ou piège**

D'une part, les FDO peuvent te demander le mot de passe qui permet de déchifrer le téléphone (si le téléphone est protégé par empreinte digitalle ou reconnaissance faciale, alors les flics l'ouvriront sans problème sans ton accord). Là tu peux :

- Refuser de donner un tel mot de passe est un délit supplémentaire mais il est rarement poursuivi s'il n'y a pas d'autre poursuite maintenue, il est relativement facile à faire annuler en cas de procès et même en cas de condamnation les peines sont légères (en général une amende de quelques centaines d'euros, sauf un cas à notre connaissance où un camarade a été condamné à de la prison avec sursis alors qu'il a été acquitté de toutes les autres accusations).

  Les FDO prétendent en général en garde-à-vue qu'ils te rendront ton téléphone si tu donnes ton mot de passe et qu'ils le conserveront dans le cas contraire, mais c'est faux comme on a pu le vérifier empiriquement avec de nombreux témoignages.

- Si en plus d'avoir chiffré ton téléphone, tu as préparé une "stratégie de déni plausible" et installé

2 Les infos contenus dans le téléphone qui peuvent être exploités par les FDO sont :
- Des « contacts » (répertoire du téléphone ou réseaux sociaux, facebook, snap) et des messages (textos ou applications, mail) et des historiques de conversation et appels (téléphone, applications)
- Des photos, vidéos et enregistrements sonores (les algorithmes dédiés et les humains reconnaissent et identifient plus facilement une personne à l'aide de sa voix qu'à l'aide d'une image de son visage. De plus, les méthodes pour « flouter » une voix sont moins efficaces que celles pour flouter une image).
- Des historiques d'applications qui renseignent sur la position du porteur (historique de Google Maps, bluetooth, historiques des wifis auxquels le téléphone s'est connecté), ses achats (Amazon) et des métadonnées de divers fichiers qui donnent également des infos de localisation notamment (à moins d'utiliser sur son téléphone des techniques particulières peu utilisées par le grand public)
- D'autres documents qui ne mettent pas en scène des personnes reconnaissables mais peuvent rendre le porteur suspect (comme un PDF des éditions la Fabrique, une brochure militante ou un plan permettant de se rendre sur un lieu occupé)

une application dédiée (comme Duress), tu peux donner aux FDO le mot de passe dit "de contrainte", qui ouvre une interface presque vide et prétend qu'il s'agit de l'interface "normale" de ton téléphone.

Le problème de cette méthode est qu'il faut être capable de résister psychologiquement aux FDO qui risque de se douter de quelque chose.

- Si en plus d'avoir chiffré ton téléphone, tu as préparé une "stratégie d'autodestruction programmée" et installé une application dédiée (comme Wasted), tu peux donner au FDO le mot de passe dit "de contrainte" qui déclenche une procédure automatisée d'effacement intégral du téléphone.

Le problème commun à ces deux méthodes (déni plausible et autodestruction par mot de passe piège) c'est que c'est une forme de désolidarisation d'avec les camarades qui refusent de donner leur mot de passe : si tout le monde refuse de donner son mot de passe, les risques de poursuite et condamnation pour ce motif diminuent (c'est vérifié empiriquement par de nombreux témoignages).

- **Résister à Cellebrite, qui court-circuite le chiffrement**

D'autre part, les FDO peuvent essayer de pomper les données avec "Cellebrite" (une probabilité désormais très élevée) ou envoyer ton téléphone à un service équipé de "Cellebrite" si eux même ne l'ont pas (probabilité plus faible).

Dans ce cas, le seul exemple qu'on a pour l'instant d'un téléphone que Cellebrite n'a pas pu ouvrir c'est un téléphone avec un mot de passe de chiffrement composé de 10 mots aléatoires, ce qui est assez pénible à utiliser au quotidien. (Voir note complémentaire II à la fin).

- **L'aide d'une personne en coulisse**

Il est possible d'installer ou de configurer en amont un moyen de déclencher à distance l'auto-effacement du contenu du téléphone. Sur Android, il y a les fonctionnalités "find my device" qui sont implémentées par défaut sur les téléphones récents[3]. Il y a une option pour déclencher à distance "la restauration aux valeurs d'usine". Il existe aussi des applications open-source comme Prey (payante pour avoir cette fonctionnalité) ou FindMyDeivce (FMD) (gratuite).

Il est aussi possible de désactiver à distance l'accès de ton téléphone aux différents services auxquels il est connecté d'habitude, comme les applications de messagerie, les mails etc. Pour le faire, un certains nombre de services nécessite une préparation en amont.

- Pour Telegram (déconseillé, voir plus bas), il faut avoir lié l'application à un ordinateur par exemple).
- Pour Signal, *a priori* la seule manière de le désactiver à distance est de commander une nouvelle carte SIM pour le même numéro de téléphone et se connecter à Signal sur un autre appareil avec la nouvelle carte SIM et débrancher à distance le Signal présent sur l'ancien téléphone depuis Signal sur le nouveau téléphone.

Si tu as bien briefé le ou la proche que tu compte faire prévenir en garde-à-vue, il ou elle peut s'occuper d'effacer à distance ton téléphone dès qu'il ou elle apprend que tu es en garde-à-vue.

Il y a de nombreux cas de figure où ça ne fonctionne pas (racket en rue notamment) et le ou la proche peut être prévenue trop tard pour effacer le téléphone avant que son contenu ne soit consulté ou copié par les

3 Une fois configuré sur le téléphone, l'adresse pour effacer à distance est https://www.google.com/android/find/

FDO.

2. Saisie du téléphone et utilisation ultérieure

Probabilité de cette menace : 4/5 à 3/5

Indépendamment de si le procureur décide de poursuites ou non à l'issue de la garde-à-vue, indépendamment de si le téléphone contient ou non des infos qui intéressent les FDO et indépendamment de si les FDO y ont déjà eu accès ou non[4], ils peuvent décider de conserver ton téléphone. Tu peux faire une demande pour le récupérer mais c'est long et arbitraire (le procureur décide seul et n'a pas à se justifier).

Si les FDO conservent ton téléphone et qu'une enquête en encore en cours, alors il y a un risque très important que les FDO continuent de réceptionner et de se servir de toutes les nouvelles infos qui arriveraient sur le téléphone même bien après la fin de la garde-à-vue. Par exemple, si des personnes continuent à t'envoyer des messages car elles ne savent pas que les FDO détiennent ton téléphone.

Si les FDO conservent ton téléphone mais qu'il n'y a pas d'enquête en cours, ce risque est minime.

Dans les deux cas, il y a un aussi risque mineur que les FDO se servent de ton téléphone pour usurpation d'identité (se faire passer pour toi pour envoyer des messages à des camarades pour les piéger par exemple) ou encore pour utiliser tes données personnelles (par exemple bancaires) pour des malversations de droit commun (genre acheter des trucs sur Amazon pour eux avec ta CB, ce qui s'est déjà vu).

Si tu as préparé ce qu'il faut avant, tu peux au moins effacer la plus grande partie de ton téléphone à distance en sortant de garde-à-vue ou quand tu retrouves l'accès à un ordinateur.

Pour être serein·e en garde-à-vue et donc ne pas avoir peur de perdre son téléphone et de devoir l'effacer et aussi pour conserver sur son téléphone le moins d'informations sensibles possibles, il peut être pertinent d'avoir sauvegardé toutes ces données à l'avance (ou automatiquement) sur des clouds à l'aide d'un chiffrement de bout en bout et open-source.

3. Logiciel espion dans ton téléphone

Probabilité de cette menace : 2/5 à 1/5

Si les FDO ne conservent pas ton téléphone après qu'ils y ont eu accès, il y a un risque mineur qu'ils y ont installé un logiciel espion avant de te le remettre. Dans ce cas, si tu continue à utiliser ton téléphone ensuite comme si de rien n'était, les FDO peuvent utiliser ce logiciel espion pour continuer à collecter des données incriminantes pour toi et les autres.

Dans ce cas, tu peux sans avoir eu besoin de te préparer à l'avance :

- réinstaller l'OS avec "la restauration des réglages d'usine" (suffisant si le logiciel est est sur l'OS, le plus probable)
- supprimer l'OS original et installer une rom custum (nécessaire si le logiciel espion est dans l'installateur de l'OS original, peu probable)
- changer de téléphone (nécessaire si le logiciel espion est dans une couche inférieure, probabilité extrêmement faible)

4 De nombreuses personnes témoignent par exemple de gardes-à-vue où certain·es donnent le mot de passe et d'autres non et où tout le monde récupère son téléphone ou l'inverse.

B - Second cas de figure : les FDO n'ont pas accès physiquement à ton téléphone

1. Réquisition de données liées au réseau GSM

Probabilité de cette menace : 5/5

- Le contenu des SMS et leurs méta-données (c'est à dire qui a envoyé quoi à qui quand et de quel endroit à quel endroit) sont stockés a priori pendant un an par les opérateurs téléphoniques et accessibles aux FDO sur simple réquisition administrative ou judiciaire (voir note complémentaire III à la fin). De même pour les métadonnées des appels, mais pas le contenu (donc seulement quel numéro a appelé quel numéro quand et où). À notre connaissance, si les FDO le demandent rarement lorsqu'ils placent en garde a vue des centaines de manifestants d'un coup, c'est en revanche le B-A-BA dans toute enquête même de base sur une personne ou une « filière ».

Pour éviter ça, idéalement n'utilise pas du tout les textos et les appels "en clair" par le réseau téléphonique et privilégies par exemple l'application Signal ou le protocol Matrix[5].

- Les antennes relais par lequel passent le signal GSM enregistrent pendant des mois le passage d'un téléphone, même en mode avion (la preuve, on peut téléphoner aux secours en mode avion), même éteint (à moins d'avoir retirer la batterie, ce qui n'est en général impossible sur les modèles récents). Et ces informations sont réquisitionnables facilement par l'autorité judiciaire. On dit qu'un téléphone a « borné » à un endroit (en fonction de la densité en termes d'antennes dans la zone, la précision du bornage peut être de quelques mètres à quelques centaines de mètres).
- Parallèlement, les FDO utilisent aussi des "IMSI catcher". C'est un appareil technique qui tient dans une malette et qui "imite" une antenne relais afin que tous les téléphones alentours s'y connectent, mais en réalité c'est un dispositif des FDO pour enregistrer "en direct" les numéros de SIM et IME (voir plus bas) des téléphones dans un rayon de X mètres autour de l'IMSI catcher et leur activité en direct par le réseau GSM (contenu et métadonnées des SMS et métadonnées des appels). Très utilisé en manif par exemple pour savoir qui est présent, surtout dans les cortèges qui gigotent un peu.
- Si une carte SIM est présente dans le téléphone et que le téléphone n'est pas en mode avion etou éteint, alors le bornage enregistre le numéro de téléphone. Impossible de prétendre sérieusement qu'on n'était pas à un endroit donné à un moment donné si sa carte SIM rattachée à son identité y a borné. Autre risque lié au bornage : si 20 personnes bornent au meme endroit et que 15 se font serrer en flagrant délit, alors les 5 autres qui ont borné au même endroit deviennent suspects.

Pour éviter cette menace probable, on peut mettre le tel en mode avion ou l'éteindre lorsqu'on se déplace en manif par exemple (attention ça ne protège pas d'autres menaces moins probables, voir plus bas).

Attention aux effets indésirables : par exemple si tou·tes les participant·es d'une réunion militante éteignent leur téléphone ou le mettent en mode avion à chaque début de réunion, alors ça permet aux FDO potentiellement de savoir qui était à cette réunion (tous les téléphones qui s'éteignent en même temps à chaque fois). Parfois, trop de précaution c'est moins bien que moins de précaution. D'une manière générale, il vaut mieux adopter des comportements "les moins stéréotypés possible" pour "brouiller les pistes" : par exemple, prendre l'habitude de mettre son téléphone en mode avion en pleine journée, ou bien que certain·es participant·es à une action mettent le téléphone en mode avion et d'autres le laissent à la maison.

---

5 Nous ne recommandons pas Telegram car seuls les "chats secrets" sont chiffrés alors qu'ils sont en réalité peu utilisés (ils ne sont pas utilisables sur ordinateur ni en groupe) et même dans ce cas les avis techniques sont plutôt défavorables à Telegram par rapport à Signal (voir note complémentaire IV à la fin).

On peut aussi avoir une SIM prépayée dédiée à l'activisme, achetée en liquide et non enregistrée pour qu'elle ne soit pas liée officiellement à son identité (ces cartes SIM ont une durée de vie limitée et implique de changer souvent de numéro de téléphone).

2. Réquisition de données liées au réseau 3G/4G/5G

Probabilité de cette menace : 4/5

Les données qui sont échangées entre un téléphone et un serveur en ligne (ses contacts téléphoniques Apple ou Android par exemple, ce qu'on fait sur un site web ou encore le contenu d'un message sur WhatsApp ou un mail) pourraient également être interceptées « en chemin » et à distance. Les FDO peuvent solliciter auprès de ton opérateur téléphonique un historique de ton activité qui sollicite les réseaux de "données mobile" (comme la 3G et la 4G).

Aujourd'hui, la quasi totalité des services en ligne (qu'on y accède par un navigateur web comme Mozilla Firefox ou une application dédiée comme Gmail) utilisent par défaut la technologie "HTTPS", qui protège le contenu des échanges entre ton téléphone et les serveurs en ligne. En revanche, ce à quoi tu te connectes, quand et d'où n'est pas protégé par HTTPS. Tu peux utiliser en permanence quand c'est possible un VPN[6] qui se charge de "masquer" également cela, mais tu n'es pas à l'abri que les FDO collaborent avec le fournisseur de ton VPN pour obtenir ces données "masquées". Si tu veux être sûr qu'elles restent secrètes, tu peux utiliser à la place et gratuitement le navigateur Tor, surtout pour tes activités les plus sensibles (on ne peut pas forcément utiliser Tor tout le temps parce que c'est lent mais c'est bien de l'utiliser aussi pour des trucs non sensibles pour "brouiller les pistes" pour soi et les autres[7]), car Tor utilise un système plus poussé qu'un simple VPN, ce qui rend techniquement impossible une éventuelle collaboration avec les FDO.

3. Criblage manuel des données publiques en ligne

Probabilité de cette menace : 3/5

Les autorités n'ont pas besoin de saisir le téléphone ni de « cracker » le chiffrement de vos communications si vous publiez publiquement en ligne des photos de manif ou si vous vantez auprès de FDO infiltrées vos exploits militants ou de ceux des autres. Aujourd'hui, les réseaux sociaux sont un terrain d'enquête privilégié des FDO qui se contentent souvent de cela pour réunir les preuves nécessaires pour faire tomber des prévenus de droit commun. Via l'utilisation de graphes sociaux, dans une certaine mesure même les photos de vacances avec X, Y ou Z alimentent les algorithmes des FDO pour savoir qui connait qui et justifient notamment des accusations de "participation à un groupement en vue de".

Tu peux essayer de garder en tête que publier publiquement une information revient à en remettre une copie aux FDO et que tu ne pourrais pas savoir si les FDO la consulte effectivement ou non. Pour réduire les risques et éviter d'alimenter la surveillance de masse, tu peux faire attention à ce que tu publies publiquement.

Tu peux aussi appliquer avec plus ou moins d'assiduité une stratégie de cloisonnement : une « identité numérique » différente pour chaque usage (un mail ou un compte de réseau social pour un groupe militant et un autre mail ou compte de réseau social pour une autre organisation par exemple). D'ailleurs, c'est aussi valable "in real life" : tu n'es pas obligé·e de décliner ton prénom ou un même surnom à chaque action ou organisation politique.

---

6 Pour une liste de VPN conseillés dans une perspective générale de sécurité de tes données : https://www.privacyguides.org/en/vpn

7 Lors de l'atelier du mois de mai, il n'a pas été tranché définitivement si l'utilisation d'un VPN permet d'éviter que les données de connexion soient enregistrées par l'opérateur téléphonique et donc consultables par les FDO.

4. Réquisition de données collectées et générées par les entreprises privées

Probabilité de cette menace : 2/5

Le contenu et les métadonnées des messages envoyés depuis les applications commerciales (comme Facebook, WhatsApp, Snapchat, Skype etc) et les métadonnées des appels effectués par ces applications sont potentiellement conservées par ces entreprises encore plus longtemps que celles conservées par les opérateurs téléphoniques. Ces données sont également accessibles aux FDO sur réquisition administrative ou judiciaire. Certains applications (comme WhatsApp) prétendent que le contenu des échanges serait « crypté » et donc non consultable par les FDO, mais rien ne permet de l'attester réellement. Même celles-ci en tout cas communiquent les métadonnées.

Pour se prémunir contre cela, éviter au maximum de donner des infos à ces entreprises privées (notamment les GAFAM et les jeux vidéos sur téléphone). Il est relativement simple de remplacer l'usage des GAFAM par d'autres applications open-source[8] et chiffrées de bout en bout[9]. En cas d'utilisation quand même des GAFAM (on fait ce qu'on peut), tu peux aussi "isoler" ces applis GAFAM du reste du téléphone à l'aide d'une application Shelter, qui fait qu'au moins les GAFAM pompent moins de données présentes ailleurs sur le téléphone.

Attention, les métadonnées générées par l'utilisation d'applications de confiance (comme Signal) sont également susceptibles d'être réquisitionnées par les FDO, bien que celles-ci leur sont beaucoup moins utiles que le contenu des messages (les FDO ne peuvent pas récupérer le contenu des messages Signal par exemple, à moins de mettre la main sur le téléphone d'une personne avec qui tu échanges, voir plus haut).

Tu peux utiliser au maximum le chiffrement des données, même pour partager des informations qui ne sont pas sensibles (comme la liste de courses de mamie), afin d'éviter que les FDO ne trouvent suspectes les communications chiffrées et d'éviter qu'elles puissent consacrer toute leur énergie à déchiffrer les rares communications chiffrées qui seraient effectivement sensibles. Récemment, dans l'affaire dite « du 8/12 », il a été reproché par le parquet et la DGSI aux prévenus d'avoir utilisé Signal. Une accusation qui n'aurait probablement plus de sens si tout le monde utilisait Signal tout le temps.

5. Enquête plus poussée sur un·e individu·e ou un·e filière

Probabilité de cette menace : 2/5 à 0,1/5

- **Surveillance en direct et écoute téléphonique**

Le recours aux écoutes téléphoniques, c'est à dire la possibilité pour les FDO d'avoir accès au contenu d'une communication téléphonique qui passe par le réseau GSM en direct (quitte à l'enregistrer pour l'écouter plus tard) est beaucoup plus encadré que la possibilité d'accéder aux textos et aux métadonnées des appels et des textos. A priori, les données qui ne passent pas par le GSM ne sont pas concernées. Pour déjouer une éventuelle écoute téléphonique et pour éviter de t'exposer à la menace de réquisition des données d'une application non chiffrée ou non open source (voir plus haut), tu peux privilégier pour tous les échanges oraux les appels Signal.

- **Recoupement entre carte SIM et numéro IME du téléphone**

Chaque téléphone possède un numéro de série (IME). Les antennes relais (et les IMSI catcher) enregistrent les numéros des cartes SIM mais aussi ces numéros de série IME. En cas d'enquête un peu plus poussée, si

8 La confiance dans les logiciels open-source vient du fait que le code informatique derrière ces logiciels est lisible par tout un chacun et qu'une armée de geeks se fait un malin plaisir à en vérifier l'honnêteté à chaque mise à jour.

9 Le chiffrement de bout en bout signifie que le codage s'effectue directement sur le téléphone qui envoie les données et qu'elles sont donc chiffrées avant même de quitter le téléphone ce qui protège d'une interception éventuelle.

une antenne a borné un téléphone sans SIM (ou avec une SIM en mode avion), les flics peuvent effectuer divers recoupements entre IME et SIM dans la base de données des autres bornages pour savoir à qui appartient le téléphone qui a borné, même si il était en mode avion ou qu'il n'avait pas de SIM.

Pour être sûr de ne pas borner mais quand même avoir son téléphone sur soi, on peut mettre le téléphone dans une « cage de faraday » artisanale, c'est à dire une boite recouverte d'aluminium (il y a plein de tutos sur Internet). A voir si certains trouvent ça plus pratique que de ne pas prendre son téléphone du tout.

Tu peux aussi avoir un téléphone dédié à l'activisme, avec une carte SIM prépayé dédiée, les deux achetés en liquide et non enregistrés pour que ni l'une ni l'autre ne soient lié·es officiellement à ton identité (il faut alors n'avoir jamais mis dans ce téléphone de SIM à ton nom).

- **Exploitation d'une brèche de sécurité pour obtenir même les données chiffrées par un logiciel open source**

Les données chiffrées par des applications de messagerie open source chiffrées de bout en bout (comme Signal) sont illisibles en l'état par les FDO qui réussiraient à les capter ou à les réquisitionner et ce chiffrement est aujourd'hui "incassable". En revanche, ces données sont déchiffrés sur ton téléphone afin que tu puisse les utiliser (par exemple, lire tes messages). Or les services ou les outils les plus perfectionnés, réservés pour l'instant aux affaires de « *terrorisme d'ultra gauche* » peuvent exploiter une "brèche de sécurité" de ton téléphone pour y accéder lorsqu'elles sont déchiffrées. Donc même en utilisant ces applications, il vaut mieux éviter d'être explicite sur les trucs les plus sensibles ou de balancer d'autres personnes.

Par ailleurs, il est consillé d'une manière générale de toujours maintenir son téléphone à jour, c'est à dire de ne jamais repousser une proposition de mettre à jour les différentes applications ou le système car "les brèches de sécurité" sont "sécurisées" après leur découverte dans la mise à jour suivante.

- **Utilisation du micro du téléphone comme "mouchard"**

Un service de renseignement peut payer une entrprise privée de cyber-sécurité pour utiliser son outil nommé Pegasus et avoir un accès illimité à toutes les données d'un téléphone d'une personne, en continu, y compris l'accès à l'appareil photo et au micro et ce sans que la personne ne soit au courant. On ne sait pas comment s'en protéger mais ce n'est probablement pas une menace sérieuse pour l'instant du fait de son coût. En 2021, la presse indiquait que 1000 français auraient été ciblés par Pegasus et que le prix de vente à un service de renseignement s'élevait à plusieurs dizaines de millions d'euros (pour un nombre indéterminé de cibles). (Voir note complémentaire V à la fin).

On ne connait pas pour l'instant d'autres outils techniques qui permettraient d'utiliser le micro du téléphone en continu pour enregistrer des conversations ou autres, à l'insu du propriétaire du téléphone. A priori vu ce qu'on sait actuellement, ce n'est pas forcément pertinent de couper tous les téléphones pour tenir une réunion car ça risque de créer un effet indésirable (voir partie sur l'exploitation du réseau GSM). En revanche, n'importe quel supplétif de FDO (comme un "indic") peut avec son smartphone décider d'enregistrer une réunion ou des propos de militant·es. Diverses pratiques pour se prémunir de certains risques d'infiltration par les FDO ou leurs supplétifs sont synthétisées dans des brochures de qualité (par exemple, décider collectivement de tenir les réunions sans smartphone présent dans la pièce).

C - Récapitulatif

1. En cas de risque de saisie physique du téléphone

Récapitulatif des conseils les plus simples à mettre en oeuvre donnés dans cette brochure face aux menaces les plus probables que représentent les FDO pour soi mais surtout pour les autres.

- Chiffre ton téléphone (ou vérifies qu'il est chiffré par défaut) et configure un mot de passe de plusieurs lettres et symboles. Ça n'empêchera probablement pas les FDO de consulter le contenu de ton téléphone, mais ça réduit grandement le risque qu'ils se servent de ton téléphone pour usurper ton identité ou qu'ils y installent un logiciel espion.

- Idéalement, plus tu prends de risque (aller en manif'action est plus "risqué" en ce sens que de tracter pour la CGT devant son entreprise) et plus ça vaut le coup de ne pas avoir de téléphone sur toi ou d'avoir un téléphone le plus vide possible (mais qui peut utiliser Signal pour ne pas utiliser le réseau GSM), soit parce qu'il est dédiée à ces activités soit parce que tu le remets à zéro avant chacun de ces activités et qui soit effaçable à distance.

- Dans tous les cas, il est conseillé de sauvegarder régulièrement tes données personnelles pour ne pas avoir peur de les perdre en cas de sasie et pour résister aux pressions des FDO.

- Briefe ton ou ta proche qui sera prévenu·e si tu es placé·e en garde-à-vue pour qu'iel puisse effacer à distance tout ton téléphone (il faut avoir configuré une application comme FindMyDevice) et désactiver le plus vite possible tes applications sensibles (comme Signal et tes mails). À défaut, occupes-t-en dès que tu sors de garde-à-vue ou que tu as de nouveau accès à un ordinateur car si les FDO conservent ton téléphone ils peuvent continuer à s'en servir après la fin de la GAV, de la perquisition ou du contrôle.

- Si les FDO mettent la main sur ton téléphone puis te le rendent, réinitialise-le à zéro pour supprimer la plupart des potentiels logiciels espions qu'ils y auraient installés.

2. À distance sans risque de saisie du téléphone

Récapitulatif des conseils les plus simples à mettre en oeuvre donnés dans cette brochure face aux menaces les plus probables que représentent les FDO pour soi mais surtout pour les autres.

- Garde ton téléphone à jour, c'est à dire ne repousse jamais une proposition automatique de mettre à jour un logiciel ou le "système" de ton téléphone pour éviter aux FDO de pouvoir exploiter certaines brèches de sécurité.

- Idéalement, plus tu prends de risque (aller en manif'action est plus "risqué" en ce sens que de tracter pour la CGT devant son entreprise) et plus ça vaut le coup de ne pas avoir de téléphone sur toi ou de mettre son téléphone en mode avion ou de retirer la batterie pour éviter que la position de ta carte SIM ne soit enregistrée par les antennes relais. Dans ce cas, évite d'adopter un comportement trop stéréotypé ou trop identique à celui de tes camarades (ne pas éteindre le téléphone au même endroit ni au même moment par exemple).

- Utilise le moins possible les SMS et les appels par le réseau GSM, qui sont très facilement accessibles par les FDO. Utilise plutôt une application de messagerie chiffrée de bout en bout et open source avec une bonne réputation, comme Signal. Pas uniquement pour les conversations sensibles mais tout le temps afin de brouiller les pistes et de ne pas alimenter la surveillance de masse.

- Utilise le moins possible les GAFAM ou à défaut les isoler dans une application Shelter car les FDO peuvent accéder à toutes les données récoltées par les applications commerciales (comme l'historique des positions Google Maps ou les photos partagées sur Messenger).

- Utilise le plus possible un VPN pour tes activités en ligne et le navigateur Tor pour tes activités les plus sensibles.

- Met en place une stratégie personnelle de cloisonnement en ligne et dans la vraie vie, c'est à dire ne donne pas la même identité partout et encore moins la vraie. Continue avec tes camarades à faire attention à ne pas communiquer d'informations sensibles à l'oral en présence d'inconnus ou dans des lieux potentiellement surveillées (comme la plupart des locaux militants publics).

- Evite quoi qu'il en soit de communiquer des informations directement incriminantes même en utilisant les meilleurs applications car les services de renseignement les plus poussés auront toujours une longueur d'avance technologique, même s'ils ne déploient leurs plus gros moyens que pour les enquêtes les plus poussées.

D - Pour aller plus loin

Ou pour comprendre plus en détails les enjeux qui justifient les conseils donnés dans cette brochure.

Notes complémentaires

I. Avec nos informations personnelles et les données générées par notre utilisation des téléphones portables, les FDO peuvent :

- montrer ou faire entendre le porteur du téléphone dans une activité illégale en soi (comme une dégradation) ou entrain de participer à une activité qui n'est pas légale à cause du contexte (comme une participation à une manifestation interdite ; et donc peuvent alors directement incriminer le porteur du téléphone. Il peut aussi s'agir d'éléments qui constitueront des « aveux » aux yeux des flics (comme un contact enregistré dans le téléphone au nom de « binome de blackbloc avec qui on nique tout » ou un message envoyé à son cousin qui dit « ouais trop bien aujourd'hui j'ai brûlé un commissariat »)
- montrer ou faire entendre le porteur dans une activité légale mais qui sera jugée « suspecte » par les autorités (comme la rédaction d'une banderole antifa) ; ces éléments peuvent servir de prétexte à une surveillance plus serrée sur le porteur (dans un cadre légal ou non) ou à des actes d'enquêtes judiciaires.
- montrer ou faire entendre le porteur dans une situation qui n'a en soi pas de sens direct mais peut compromettre sa défense (par exemple, prétendre qu'il a passé la manif dans le cortège syndical alors qu'une photo dans son téléphone le montre dans le cortège de tête).
- montrer d'autres personnes dans les activités mentionnées ci-dessus et les incriminer ou justifier le renforcement de leur surveillance ou réduire leur marges de manœuvre en termes de défense. Par ailleurs, les messages peuvent constituer des « aveux » rédigés par d'autres personnes (si votre téléphone contient un message envoyé par votre cousin qui se vante d'avoir brûlé un commissariat)
- représenter ensemble plusieurs personnes, permettant alors aux autorités d'affiner leur « graphe social » : menace réelle et anciene des flics mais désormais assisté par des algorithmes etc, ca consiste à relier entre eux des personnes (X connaît Y qui connaît Z donc c'est comme si X connaissait Z ou encore X est allé à la même manif que Y qui lui est allé combattre au Rojava avec Z qui est un terroriste) pour justifier des actes d'enquête, de la surveillance plus ou moins légale etc.

II. A priori Cellebrite n'utilise pas de backdoor Apple ou Google, donc pas d'intérêt d'installer une rom custom spécifiquement pour résister à Cellebrite, sauf un cas que pour l'instant Cellebrite ne sait pas ouvrir c'est la rom custom Graphen Os installée sur un téléphone Pixel derni-re version avec quelques conditions complémentaires, en tout cas selon leur documentation technique qui a fuité en ligne en mai 2024.

III. Sur la conservation des SMS par les opérateurs :https://www.lefigaro.fr/actualite-france/2011/11/15/01016-20111115ARTFIG00716-comment-la-police-espionne-les-sms.php

IV. Sur les limitations techniques de Telegram : https://x.com/mer__edith/status/1788687092106567694 (boss de Signal) https://x.com/matthew_d_green/status/1789687898863792453 (prof de crypto)

V. Sur le coût de Pegasus pour les services de renseignement : https://www.humanite.fr/social-et-economie/pegasus/surveillance-pegasus-le-logiciel-espion-vendu-a-60-pays-du-maroc-au-mexique-714828

Ressources complémentaires

- Guide d'autodéfense numérique du Boum : https://guide.boum.org/ ou de Camarade : https://camaraderevolution.org/index.php/2023/10/06/defense-numerique/
- Se rendre à une session ouverte du Fuz à Montreuil pour configurer son téléphone : https://wiki.fuz.re/
- Suivre une formation comme celles de NothingToHide https://nothing2hide.org/fr/nos-formations/