FADETTES, UFED ET DONNÉES DE CONNEXION

SUR LES TECHNIQUES D'INVESTIGATION NUMÉRIQUES DE LA POLICE

version 1 – Octobre 2022

L'idée de ce texte est de répondre pratiquement aux questions de sécurité numérique qu'on se pose dans les milieux militants. Il a pour but de donner des arguments aux personnes qui, dans chaque groupe, répètent qu'il faut faire gaffe à la sécurité numérique, et d'en donner aux personnes qui les trouvent reloues.

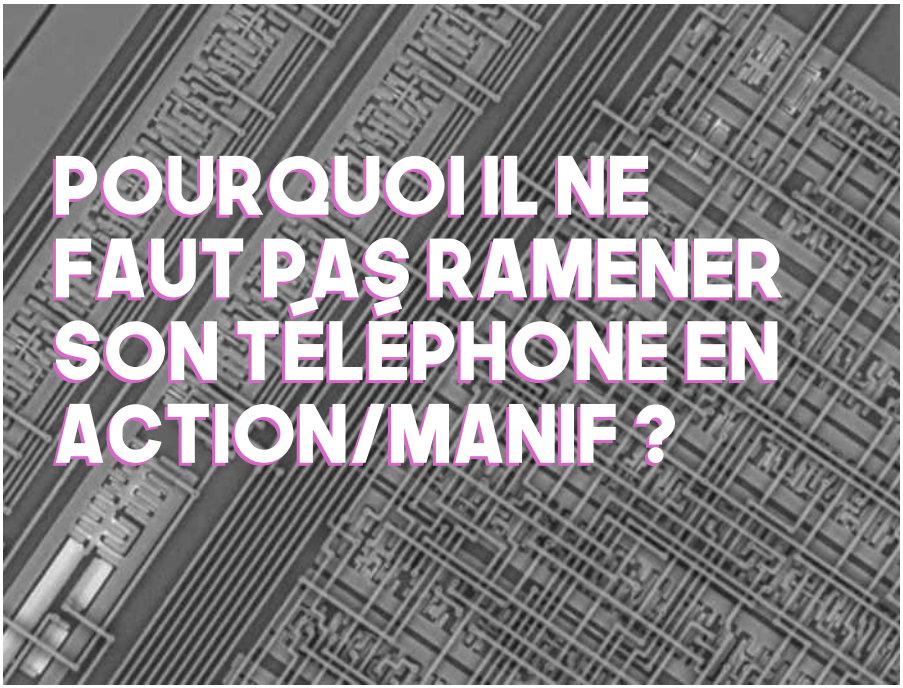
On part du constat qu'il y a un manque d'informations disponibles sur les techniques d'enquêtes que les keufs utilisent pour fouiller nos téléphones et nos ordinateurs, et sur celles qui utilisent notre navigation internet et nos communications téléphoniques. Les formations à la sécurité numérique dans nos milieux sont souvent un peu trop théoriques. Elles apportent les réponses, mais ne montrent pas les problèmes.

On se concentre donc, dans ce texte, sur les techniques d'enquêtes qui touchent nos outils numériques : analyse des données de téléphonie, écoutes, analyse de la navigation internet, analyse des données enregistrées sur nos ordis ou nos téléphones, ... On se base sur des techniques qu'on a vu être utilisées par les policier.es (contre nous, contre des potes, ou des pratiques qu'on a vues dans des documentaires).

On veut donner dans ce texte des pratiques de sécurité numérique qu'on voudrait voir généralisées dans nos milieux. On n'a pas vocation à se perdre dans des détails techniques, mais à détailler les techniques policières au maximum. Pour plus de détails sur les pratiques numériques pour se protéger face à la répression, il existe déjà plein de ressources, qu'on citera et qu'on vous invite à consulter !

version 1 – octobre 2022

Pour nous contacter, nous poser des questions, nous aider à mettre à jour cette brochure : apt-getinstall@riseup.net



Pour deux raisons principales, qu'on va détailler : déjà, c'est donner plein d'armes aux enquêteurices pour te retrouver si une enquête est ouverte sur l'action ou la manif, et ensuite, c'est risquer de se faire choper avec son téléphone.

Quels sont les risques si je me fais choper avec mon téléphone ?

Si tu pars en garde à vue avec ton téléphone, les policier.es ont de nombreuses possibilités pour exploiter les données qu'il contient. Les commissariats – surtout en Île-de-France –, commencent à être équipés d'aspirateurs à données[1], des outils qui connaissent des failles de sécurité de milliers de modèles de téléphones et de versions de systèmes d'exploitation[2] (iOs, Android ou LineageOs par exemple). Avec ces failles, l'aspirateur va copier l'entièreté des données stockées sur le téléphone et les trier pour les rendre lisibles facilement par la police. Les flics peuvent donc avoir accès à nos historiques internets, nos photos, nos documents, nos sms, la liste de nos appels, nos messages sur certaines applications (Instagram et facebook, par exemple, mais pas

1. L'utilisation d'aspirateur à données est encadrées par cet article de loi : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000029759893
2. Un système d'exploitation, c'est un « *logiciel gérant un ordinateur* [ou un téléphone], *indépendant des programmes d'application mais indispensable à leur mise en œuvre* » (Wiktionnaire)

Signal), notre historique de localisation. Aujourd'hui, les données stockées sur des téléphones récents (et sur l'entièreté des iPhones) sont chiffrées. Pour empêcher que leurs données soient exploitées, il faut qu'ils soient éteints au moment du début de l'analyse. Mais un téléphone dont le stockage est chiffré et éteint n'est pas une barrière infaillible : sur certains téléphones dont les données sont chiffrées, des failles de sécurité sont connues. On peut limiter ce risque en installant les mises à jour de sécurité des systèmes d'exploitation.

Toutes ces données sont très utiles aux keufs, qui sauront certainement y trouver des éléments directement incriminants ou des éléments permettant de montrer que vous êtes un.e turbogauchiste (genre vos notes contenant les 50 meilleures citations de Bakounine, vos selfies devant le mur des Fédéré.es, et les j'aime que vous avez laissé en 2018 sur la page Facebook de désobéissance écolo paris).

CELLEBRITE & SIGNAL_ En France, la police nationale utilise principalement des appareils de Cellebrite, les UFED, qui a récemment annoncé pouvoir avoir accès, grâce à ces aspirateurs, aux messages envoyés sur Signal. Il s'est avéré que c'était un coup de com' : Cellebrite pouvait avoir accès aux messages Signal à la condition que le téléphone soit déverrouillé. Normalement donc, les messages Signal ne peuvent pas être récupérés par les policier.es via les aspirateurs à données.

Un autre moyen d'action des policier.es en garde à vue, qui semble arriver plus fréquemment que l'utilisation d'aspirateurs, c'est de vous demander votre code de déchiffrement de téléphone, ce qui leur donne accès aux données du disque dur. Refuser de le donner est un délit – puni de 3 ans de prison et de 370 000 euros d'amende[1]. Il faut noter que ce délit ne s'applique qu'aux codes permettant de déchiffrer des données, donc, par exemple, les codes de déverrouillage de téléphones dont le stockage est chiffré. Ne pas donner un code de déverrouillage d'un téléphone non chiffré n'est pas un délit, puisque ce code n'est qu'un blocage « graphique » de l'accès au téléphone. C'est bien sûr beaucoup mieux d'avoir un téléphone chiffré puisque le risque de répression pour ce délit est faible. Le mieux reste de ne pas amener son téléphone en manif ou en action.

L'analyse de carte SIM est une technique un peu vieillote, mais elle est probablement toujours utilisée : en insérant la carte SIM dans une machine spéciale, sans avoir besoin du code PIN, les policier.es ont généralement accès au contenu des SMS envoyés, et au répertoire des contacts.

Se faire choper avec son téléphone, c'est aussi risquer que celui-ci soit placé sous scellé, qu'il soit confisqué pour être exploité pendant l'enquête ou par punition, et ça, c'est relou parce qu'il ne sera probablement jamais restitué, et s'il l'est, ce sera après un bon bout de temps et de nombreuses démarches.

1. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032654251. Les peines indiquées sont les peines maximum encourues, et ne sont jamais appliquées telles quelles

Avoir son téléphone en action permet-il aux keufs de me retrouver ?

En dehors des cas où on s'est malheureusement fait choper en flagrant délit, le fait d'avoir son téléphone pendant qu'on commet des délits donne plusieurs leviers d'enquête aux policier.es.

Les policier.es peuvent en effet avoir facilement accès à tout un tas d'informations sur les téléphones qui ont borné à l'endroit de l'action – il leur suffit pour cela de demander une autorisation à un.e procureur.e de la République, d'envoyer uner réquisition aux opérateurs téléphoniques, même Roger du commissariat de Montigny-le-Bretonneux peut le faire. Iels peuvent demander la liste des numéros IMSI (un numéro IMSI, c'est un numéro associé à notre ligne téléphonique, il identifie un contrat téléphonique) des téléphones ayant borné sur une antenne relais donnée (borner, ça veut dire que le téléphone a signifié sa présence à l'antenne relais en question : « coucou, je suis là, donne-moi du réseau », un téléphone borne très régulièrement. Précisons qu'un téléphone borne aux antennes relais à proximité de lui dès qu'il a une carte SIM insérée et que le mode avion est désactivé). La liste des personnes ayant borné près du lieu d'une action est pour la police une liste de potentiels suspects.

Pour illustrer l'utilisation que peuvent en faire les keufs, on a glané un exemple dans des documentaires en immersion avec la police sur youtube[1]. Les keufs enquêtent sur un cambriolage dans un hangar de stockage. Ils demandent la liste des numéros IMSI ayant borné sur l'antenne relais la plus proche du hangar. Plus tard dans l'enquête, ils découvrent que les suspects se sont retrouvés à tel péage plus tard dans la soirée du cambriolage. Ils demandent donc la liste des numéros ayant borné près du péage en question à l'heure dite et identifient les suspects comme étant les utilisateurs des numéros de téléphones ayant borné à ces deux endroits dans la même soirée.

Après avoir identifié les numéros suspects, Robert du commissariat de Montigny-le-Bretonneux peut de nouveau envoyer une réquisition aux différents opérateurs téléphoniques pour leur demander une identification de ligne, dans le but d'obtenir le nom et l'adresse de la personne qui paye pour le forfait du numéro IMSI en question. C'est là que ça peut servir d'avoir un forfait Lycamobile qu'on ne relie pas à notre identité LIRE QUESTION « EST-CE UTILE D'AVOIR UN BIGO AVEC UN FORFAIT LYCA ? ».

À partir de là, Robert peut entre autres envoyer une troisième réquisition dans lequel il peut demander les fadettes de la ligne. Les fadettes, pour factures détaillées, c'est un document qui récapitule la liste des bornes téléphoniques auxquelles ton téléphone a borné, pour faire plein de trucs avec (trouver où tu habites réellement, identifier des complices). Robert peut aussi faire une demande de suivi en direct de tes bornages[2] et les recevoir sur son ordi (mais, pour le coup, Robert peut pas forcément le faire, parce qu'il a probablement pas reçu la formation pour utiliser le logiciel de suivi en direct, Deveryloc),

1. https://www.youtube.com/watch?v=J4wYYXKEX_0
2. Liste de l'ensemble des réquisitions que Robert peut faire aux opérateurs : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000041553495

ce qui peut lui permettre de t'interpeller facilement. Les fadettes, elles, donnent les données pour une période que précisent les keufs, et ne permettent donc pas d'exploitation « en direct ».

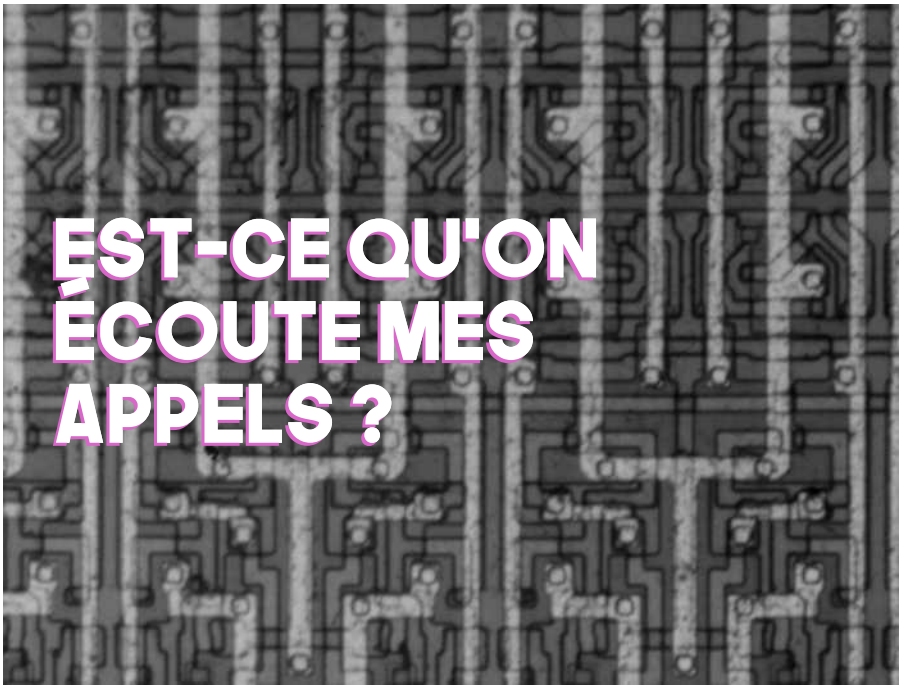
LES FADETTES… Pour en parler plus en détails, les fadettes sont des fichiers excels de milliers de lignes qui listent dans l'ordre chronologique les antennes relais auxquelles la ligne téléphonique observée a borné, les communications qu'elle a eu (appels, SMS, MMS, données mobiles), et le numéro IMEI (numéro de série du téléphone portable) du téléphone sur lequel est utilisée la carte SIM. Les fadettes sont donc une successions de localisations. Les policier.es les analysent à l'aide du logiciel Mercure, qui rend « lisibles » ces données. Les fadettes peuvent-être utilisés de nombreuses manières dans des enquêtes :

- Elles peuvent mettre en évidence des complicités : en comparant des fadettes entre elles, les policier.es peuvent savoir si des téléphones ont borné aux mêmes endroits aux mêmes moments, autrement dit, que les personnes qui les utilisent se sont rencontrées.
- Elles permettent de retrouver des trajets effectués
- Elles permettent d'identifier les contacts réguliers de l'utilisateur. Quand un.e enquêteur.ice enquête sur plusieurs personnes, iels peut tracer une carte de leurs contacts, savoir si elles sont entre elles souvent en relation, établir quels sont leurs contacts communs, …
- Elles permettent d'observer les lieux que fréquente un individu. Dans une enquête en Île-de-France où un propriétaire porte plainte pour vol et dégradations après un squat dans sa propriété, les policier.es ont demandé les fadettes de personnes, dont elles avaient déjà les identités, susceptibles d'avoir fréquenté le squat. Avec Mercure, elles ont récupéré le pourcentage de temps où les lignes téléphoniques bornaient à proximité du squat. Lea proc a décidé de poursuivre les utilisateurices des lignes téléphoniques qui ont borné près du squat entre minuit et 6h du matin : c'est-à-dire des personnes qui y dormaient. Les fadettes permettent, de la même façon, de confirmer l'adresse d'une personne.

La police peut aussi travailler ces données dans « l'autre sens » : plutôt que de chercher des suspects, elle peut les utiliser pour confirmer la culpabilité de gens qu'elle soupçonne. Robert suspecte quelqu'un.e d'avoir commis un crime ou un délit, il peut, à partir de son identité, de son numéro IMSI, ou de son numéro IMEI, demander à chacun des opérateurs téléphoniques si cette information est rattachée à un contrat, avant de demander les fadettes du contrat en question.

Une décision récente de la cour de cassation[1] limite l'utilisation de ces données et leur conservation par les opérateurs. Jusqu'ici, les données étaient conservées 1 an, et étaient accessibles aux policier.es pour n'importe quel type d'enquête. Dorénavant, les données de connexion et de localisation (c'est-à-dire de bornage) ne seront plus accessibles aux enquêteur.ices pour les enquêtes portant sur des « *infractions ne relevant pas de la criminalité grave* ». Leur usage sera (un peu) limité pour la criminalité grave (en gros, des faits de « *meurtre en bande organisée, destruction par moyen dangereux, importations et exportations de centaines de kilos de stupéfiants par organisation criminelle de dimension internationale, etc.* »).

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



C'est tout à fait possible. En France, il y a deux types d'écoutes téléphoniques. Les écoutes judiciaires et les écoutes administratives (de renseignement)[1].

Pour les écoutes judiciaires, elles sont limitées aux faits de « délinquance organisée » et aux crimes. Elles sont décidées, dans le cadre d'enquêtes de flagrance ou d'enquêtes préliminaires[2], par un juge des libertés et de la détention, et, dans le cadre d'informations judiciaires, par le juge d'instruction. Ces écoutes sont limitées dans le temps (1 mois renouvelable 1 fois pour les enquêtes préliminaires et pour les enquêtes de flagrance, et 4 mois renouvelables 5 fois au maximum, et pour certains crimes seulement, dans le cadre des informations judiciaires).

Les écoutes administratives, elles, sont autorisées par lea premier.e ministre sur proposition des services de police ou de renseignement. Elles ne concernent donc pas une enquête en particulier, il n'y a pas besoin de suspecter la personne d'avoir commis un

1. Le cadre légal des écoutes est défini dans ces articles de loi: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039279192 et https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000044568189
2. L'information judiciaire, l'enquête de flagrance et l'enquête préliminaire sont trois différents types d'enquêtes. La première est menée par un juge d'instruction, concerne toutes les affaires de crimes, mais peut aussi être ouverte pour enquêter sur des délits complexes. Elle donne des droits étendus aux enquêteurices. L'enquête de flagrance concerne les « flagrants délits », elle est menée par un Officier de Police Judiciaire (OPJ), sous le contrôle d'un procureur. Il en va de même pour l'enquête préliminaire, dans laquelle les possibilités des enquêteurices sont limitées.

LA DÉLINQUANCE ORGANISÉE… La délinquance organisée, n'est pas un concept défini clairement, mais il regroupe tous les délits commis « en bande organisée » ainsi que, entre autres, les crimes de destruction et de dégradations en bande organisée (souvent utilisé lors de manifestations), de détournement d'aéronef, de terrorisme, et les délits très vagues d'association de malfaiteurs (qui a déjà été utilisé contre des groupes anarchistes), et d'atteinte aux intérêts fondamentaux de la nation. Cette liste de délits[1] est celle pour laquelle les enquêteurices peuvent utiliser les « techniques spéciales d'enquête », comme les écoutes téléphoniques, comme l'installation de logiciels espions sur les smartphones et les ordinateurs.

délit pour la mettre sur écoute. Elles servent au renseignement. L'autorisation de lea premier.e ministre est valable 4 mois, et elle est renouvelable sans limite.

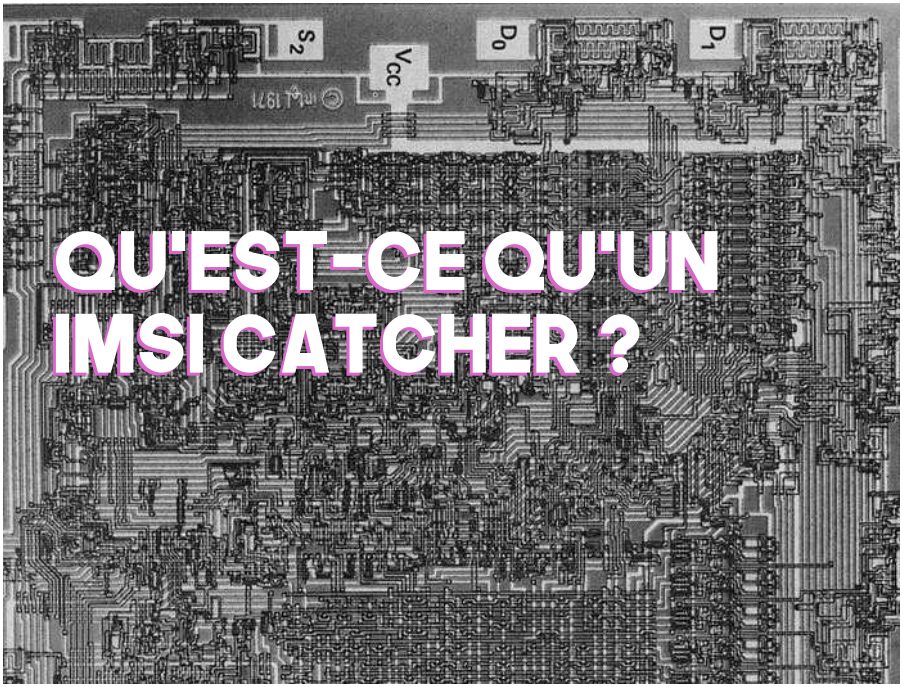
Les écoutes téléphoniques ne se restreignent pas à l'écoute des appels téléphoniques. Théoriquement, elles incluent l'interception de toutes les « correspondances téléphoniques », y compris, par exemple, les appels et les messages Signal. Si les policier.es ne peuvent y avoir accès, ce n'est donc pas pour des raisons légales mais simplement pour des limites techniques : les policier.es ne parviennent pas à déchiffrer les communications via Signal. Les SMS sont donc aussi sujets aux écoutes téléphoniques, et les écoutes sont une pratique courante de la police et des services de renseignement. Les informations communiquées par SMS peuvent donc très facilement être interceptées. Enfin, en mettant en place des écoutes téléphoniques, les policiers ont connaissance des pages web que l'utilisateur consulte en utilisant ses données mobiles. Utiliser Tor **LIRE QUESTION « POURQUOI DEVRAIS-JE UTILISER TOR ? »** sur son téléphone est un moyen de détourner l'espionnage via les écoutes téléphoniques, des pages web consultées.

En France en 2018, l'année des gilets jaunes, 22 000 personnes ont été placées sur écoute. 9 % de ces écoutes concernaient des faits de « violences collectives », donc, en gros, « d'émeute ».

1. La liste complète des délits et crimes concernées se trouve ici : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042919831 et ici : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311624

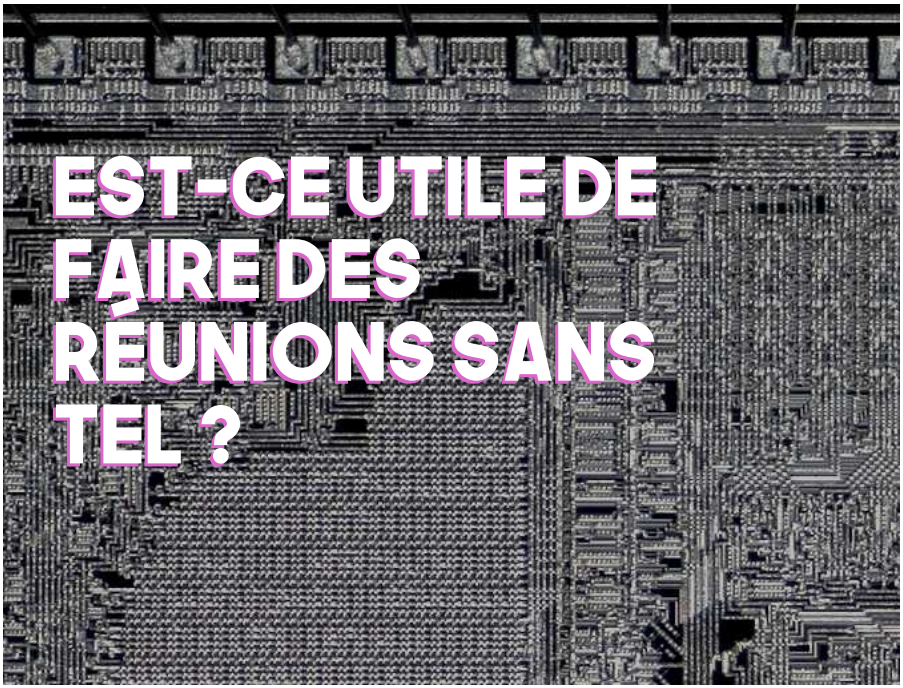
Ça dépend vraiment de ce qu'on a à cacher. Un bigo n'est pas fait pour dissimuler des informations. Pour cela, Signal marche beaucoup mieux. Un bigo, ça envoit des SMS, ça passe des appels, que les policier.es peuvent tout à fait intercepter dans le cadre d'écoutes téléphoniques. Si, par contre, on cherche à cacher notre identité, avoir un forfait Lycamobile (ou autre) qu'on a acheté et installé sans donner notre identité est la seule solution efficace. Légalement, il est obligatoire qu'un forfait téléphonique soit relié à une identité, et, à part dans des magasins Lycamobile pas trop regardants, c'est difficile d'échapper à cette obligation. Par exemple, pour préparer une action, c'est contre-productif d'utiliser un bigo. Mieux vaut ne pas en parler via des téléphones/ordinateurs, ou, au pire, en parler via Signal. En parler par messages normaux, c'est risquer l'interception des informations. Par contre, pour communiquer pendant une action, le bigo peut-être utile. Il n'en demeure pas moins qu'on risque de se faire choper avec le bigo, et donc que le mieux reste de ne pas en avoir. On peut sinon préparer des moyens rapides de casser le bigo et la carte sim pour les rendre inexploitables.

Utiliser simultanément et transporter ensemble un bigo anonyme et un téléphone relié à notre identité met en danger l'anonymat du bigo. Les keufs regardent souvent les numéros de téléphones qui bornent aux mêmes endroits et aux mêmes moments que les bigos sur lesquels ils enquêtent, et si deux numéro apparaissent souvent ensemble, ils n'hésitent pas à attribuer le bigo au titulaire du numéro.



Un IMSI Catcher, c'est un dispositif d'écoute téléphonique qui fonctionne en se faisant passer pour une antenne relai. Les téléphones portables utilisés aux environs de l'IMSI Catcher s'y connectent, croyant se connecter à une antenne relai. L'IMSI catcher identifie donc le numéro IMSI de tous les utilisateurs présents autour de lui. Et il rend accessible à la police les SMS que les téléphones utilisés aux alentours envoient, les appels qu'ils passent, et les sites qu'ils consultent via les données mobiles. Les IMSI Catcher peuvent être utilisés dans les enquêtes pour des faits de délinquance organisée **LIRE L'ENCADRÉ « DÉLINQUANCE ORGANISÉE »**[1]. Les IMSI Catcher sont par exemple régulièrement utilisés lors des rassemblements et des festivals autour de Bure, lieu de lutte antinucléaire. Ils permettent d'identifier très rapidement un grand nombre d'individus que la police considère comme suspects et permet de capter en direct leur communications. L'usage d'un IMSI Catcher pour intercepter les communications téléphoniques peut être autorisé par un procureur de la République en cas de « *risque imminent* [...] *d'atteinte grave aux personnes ou aux biens* », donc, entre autres, de manifestations. Le collectif la quadrature du Net a découvert que des IMSI Catcher ont étés utilisés dans des manifestations parisiennes par la préfecture de police de Paris. Leur usage est limité à certains types d'enquêtes, dont celles pour destruction et pour dégradations en bande organisée, détournement d'aéronef, terrorisme, et celles pour les motifs très vagues d'association de malfaiteurs, et d'atteinte aux intérêts fondamentaux de la nation.

1. Sur les règles d'utilisation des IMSI Catcher : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032631879/2016-06-05



Oui. Dans les pratiques qu'on a précédemment listées, qui sont les pratiques courantes de la police, aucune ne permet d'écouter ce qu'entendent en permanence les micros de téléphones. Au mieux, avec les écoutes téléphoniques, les policier.es peuvent écouter nos appels, mais c'est tout. Dans certains cas pourtant, les keufs peuvent aller plus loin. Les services de renseignement (DGSE, DGSI[1], direction du renseignement de la préfecture de police...) peuvent installer – et ils le font – des logiciels espions sur les ordinateurs et lestéléphones portables, dont les capacités sont plus ou moins grandes.

Parmi les plus efficaces de ces logiciels espions, Pegasus a fait beaucoup parler de lui : développé par la société israélienne NSO, utilisé par plusieurs services de renseignement, il permet, tout en étant quasiment indétectable, d'avoir accès aux touches clavier des utilisateurs espionnés, d'avoir accès à tous les messages (même chiffrés) envoyés et reçus, d'activer les caméras et le micro du téléphone (donc pouvoir entendre et filmer toute la vie de l'utilisateur du téléphone), de faire des captures d'écrans en temps réel et de récupérer les données GPS et de localisation. C'est une menace énorme. Difficile de cacher quoi que ce soit à Pegasus. Il peut être installé à distance, sans accès physique au téléphone, et même sans aucune action de l'utilisateur

1. La DGSI (Direction Générale de la Sécurité Intérieure) est un service « *chargé de rechercher, centraliser et exploiter le renseignement intéressant la sécurité nationale ou les intérêts fondamentaux de la nation* » (Wikipédia). Elle naît de la fusion de plusieurs services de renseignements, dont les renseignements généraux, chargés du renseignement de terrain, et compte plus de 3 000 policiers.

espionné. Il utilise des vulnérabilités « zero-day » d'Android ou d'iOs, c'est-à-dire des failles de sécurité n'étant pas connues des développeureuses ou n'étant pas encore corrigées. Ces failles s'achètent, et leur coût est très élevé, une seule attaque coûterait jusqu'à 25 000 €, ce qui limite l'utilisation de Pegasus ou des logiciels espions du même type. De plus, la quantité de données captées rend compliquée et coûteuse leur exploitation (ce sont potentiellement des centaines d'heures d'enregistrement audio ou vidéo qui sont à analyser). Les logiciels type Pegasus sont donc rarement utilisés, et, quand ils le sont, c'est de manière très ciblée. Mais les risques pour l'utilisateurice d'un téléphone infecté par Pegasus sont énormes.

Les services de renseignement français n'ont pas utilisé et n'utiliseraient pas Pegasus, mais la DGSI dispose légalement de logiciels permettant un piratage à distance des téléphones, moins compétents, sans doute, que Pegasus, mais qui restent une forte menace. Au cours de l'année 2015, des logiciels espions type Pegasus auraient étés utilisés 5 fois par la DGSI[1].

LES LOGICIELS ESPIONS ET LE DROIT… Depuis 2017, et la promulgation d'une énième loi anti-terroriste qui renforce le champ d'action des services de renseignement, il est légal de recourir *« à la mise en place d'un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques »*[2] Traduisons : les keufs ont le droit, dans certains cas précis, d'accéder via des logiciels espions aux données stockées sur un téléphone (ou un ordinateur), de prendre des captures d'écran, et d'enregistrer toutes les touches clavier de l'utilisateurice.
Ces techniques d'enquêtes peuvent être utilisés pour des faits de délinquance organisée **(LIRE L'ENCADRÉ « DELINQUANCE ORGANISÉE »)**. Un service spécialisé – le Service technique national de captation judiciaire (STNCJ) – de la DGSI est chargé de mener ces enquêtes et de mettre en place les dispositifs techniques pour les permettre. Il compterait 20 employés[3].

Garder des téléphones dans des réunions où l'on échange des informations confidentielles ou compromettantes est une prise de risque, un risque peut-être faible, mais, puisque ça coûte rien de mettre son téléphone dans une autre pièce ou un peu loin, autant le faire.

L'écoute de la réunion via un logiciel espion n'est, du reste, pas le seul danger potentiel. Dans des réunions publiques, un RG, ou un indic peut très bien allumer son dictaphone et enregistrer l'entièreté de la réunion, et demander aux participant.es de mettre les tels à un endroit reste déjà une première barrière pour éviter ça.

Un troisième risque potentiel du téléphone en réunion – on n'a pas trace d'utilisation réalisée – est celui de l'observation des bornages téléphoniques. Si un groupe est ciblé par une enquête pour association de malfaiteur.ices, les policier.es peuvent observer que les membres se

1. *Investigations & téléphonie mobile. Guide à l'usage des avocat.es*, p. 64
2. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311624
3. https://www.lemonde.fr/pixels/article/2017/11/14/justice-les-enqueteurs-pourront-bientot-utiliser-des-logiciels-espions_5214397_4408996.html

réunissent régulièrement ensemble, puisqu'ils bornent le temps des réunions aux mêmes endroits. La solution serait donc d'éteindre son téléphone avant d'arriver sur le lieu de la réunion, voire d'y aller tout simplement sans téléphone.

On l'oublie un peu trop souvent, mais les services de renseignement ont aussi le droit d'installer des logiciels espions sur les ordinateurs. De même que pour les téléphones, les keufs ont alors accès à toutes les frappes clavier de l'ordinateur (dont les mots de passe), iels pourront faire des captures d'écrans en temps réel, avoir accès à la webcam, et au micro de l'ordinateur. Tout comme pour les téléphones, il faut éviter de faire des réunions séditieuses avec son téléphone sous la main. Il est donc logique d'éloigner aussi son ordinateur des lieux de réunions, de ne pas dire de dingueries devant lui.

QUELS MOYENS EMPLOIE LA DGSI ?… Il est impossible de savoir quels moyens la DGSI emploie véritablement contre les milieux militants. Il est théoriquement possible qu'elle mette en place une surveillance passive très importante – utilisant des algorithmes pour identifier des comportement suspects parmi un grand nombre d'individus, pour cartographier leur contact, pour évaluer leur dangerosité aux yeux des services de renseignement, pour ajouter des personnes à la liste des personnes surveillées, … Vu le nombre d'actions qui réussissent, et le nombre d'enquêtes qui n'aboutissent pas, on peut supposer que les services de renseignement ne nous soumettent pas à un contrôle trop assidu. Il ne faut pas mythifier les services de renseignement. La DGSI ne peut pas tout faire. Sur les questions numériques, elle est limitée par le cadre légal du renseignement[1], par ses capacités techniques loin d'être miraculeuses, et par le coût de la mise en place des moyens techniques de renseignement. Il ne faut pas surestimer la DGSI, il ne faut pas non plus oublier qu'elle a mené et permis de nombreuses enquêtes antiterroristes contre les milieux autonomes ou anarchistes.

Y'A MOYEN DE RÉSUMER SUR LES TÉLÉPHONES ET LA TÉLÉPHONIE ?

Les condés peuvent, sans accès physique à notre téléphone :

- obtenir la liste des endroits où un numéro de téléphone a borné, et donc retracer sa localisation, et ce sur un an, via les fadettes
- suivre notre position en direct
- obtenir la liste des numéros de téléphone ayant borné à un endroit donné à un certain moment, via les fadettes
- obtenir la liste des numéros qu'un.e utilisateur.ice contacte par sms ou par appel
- trouver, à partir d'un numéro de téléphone ou d'un numéro IMEI l'identité de son propriétaire
- et réciproquement, trouver, à partir d'une identité, les numéros de téléphones associés
- écouter nos appels et lire nos sms, via les écoutes téléphoniques
- plus rarement, les policiers peuvent installer des logiciels espions capables de récolter notre localisation ou d'écouter ce qu'entend le micro d'un téléphone, de prendre des captures d'écran en temps réel, d'analyser toutes les frappes clavier.

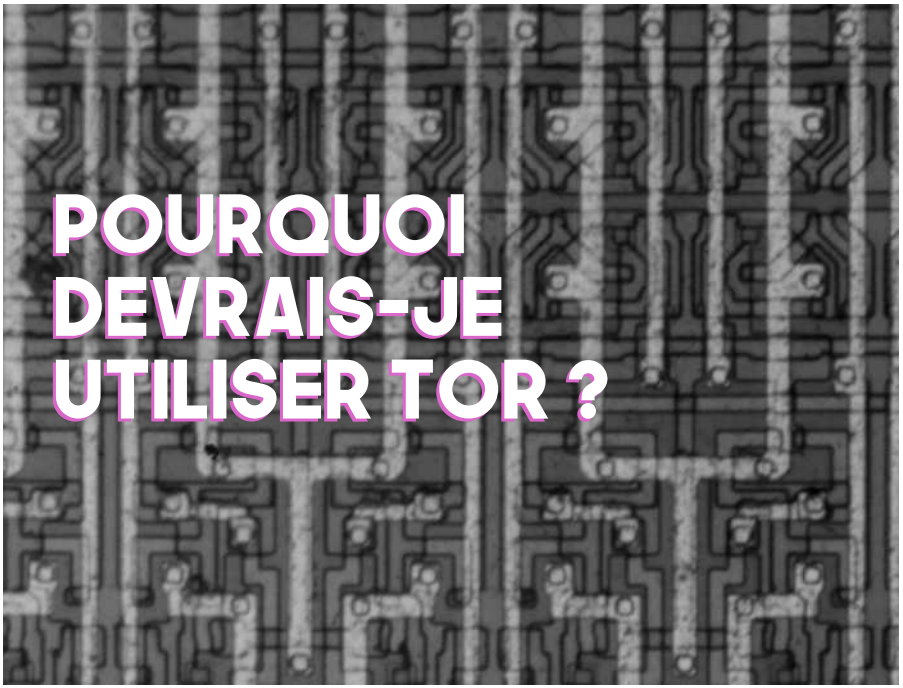
Et les policiers peuvent, avec un accès physique au téléphone ou à la carte SIM :

- avoir accès aux données stockées sur nos téléphones (photos, documents, musiques, localisation)
- avoir accès aux données stockées sur nos cartes SIM (historique des appels, contenus des sms, contacts)

1. Le cadre légal encadrant le renseignement : https://www.cnctr.fr/3_cadre_legal.html

Oui. Et pas qu'un peu. Ces deux applications de messageries chiffrées n'ont pas du tout les mêmes niveaux de sécurité. Sur Signal, tous les messages sont chiffrés de bout en bout, c'est-à-dire qu'à l'exception des personnes qui communiquent, personne ne peut les lire « en clair ». Sur Telegram, seul les Secret Chat sont chiffrés de bout en bout, et il n'est pas possible de faire de conversation de groupe chifrée de bout en bout. Le « programme », le code source de Telegram est par ailleurs propriétaire (il appartient à quelqu'un et n'est pas publiquement accessible), ce qui, en plus d'être sacrément nul politiquement (la propriété, c'est du vol), rend difficile une véritable évaluation de sa sécurité : le code n'étant pas publiquement consultable, des observateurices extérieurs ne peuvent pas y trouver les défaillances dans la sécurité. Telegram enregistre sur ses serveurs l'entièreté des messages et des médias envoyés. Et on a donc vu que Telegram peut avoir accès à ces données « en clair ». Théoriquement, les services de police peuvent demander eux aussi l'accès à ces données, mais il semble que Telegram refuse de collaborer avec eux et de répondre à leurs réquisitions.

Signal n'enregistre sur ses serveurs que les données essentielles à son utilisation : le numéro de téléphone, la date et l'heure de création du compte et la date et l'heure de la dernière connexion au compte. Signal est un logiciel libre (il n'est la propriété de personne, le code source peut-être modifié et réutilisé), dont le code source est accessible et est vérifié par des observateurices extérieurs. Vu que le code est public, le créateur ne peut pas y mettre des portes dérobées (c'est-à-dire des accès cachés aux données), ou des codes malveillants. Les failles de sécurité sont très accessibles et donc vite corrigées.



À chaque fois que quelqu'un.e navigue sur internet, iel se voit attribuer une adresse IP. Notre ordinateur échange des données, c'est-à-dire des informations, avec le serveur du site recherché : comme avec nos adresses postales, les adresses IP permettent aux serveurs, et à notre ordinateur, de communiquer entre eux. On navigue sur internet via un fournisseur d'accès (FAI, genre Orange ou Free), qui est légalement obligé de conserver des données permettant de relier chaque adresse IP à l'identité de celui qui l'a utilisé. Les hébergeurs de contenus publics sur le web (comme blogspot, qui héberge des blogs, ou les services de mail), doivent eux conserver chaque adresse IP ayant « *contribué à la création d'un contenu mis en ligne* », donc par exemple l'adresse IP d'un individu ayant publié un article sur un blog, l'adresse IP avec laquelle une adresse mail a été créée, ou les adresses IP se connectant à une adresse mail. En plus de ces données qu'ils doivent conserver, les hébergeurs en conservent d'autres, pour leur fonctionnement ou pour revendre des données personnelles. La police peut demander l'accès à ces données, et obtient donc, d'un côté, une adresse IP, et de l'autre, un moyen d'associer une identité à cette adresse IP. Combinées, ces informations lui permettent d'identifier l'auteur d'un contenu mis en ligne.

Par ailleurs, les Fournisseur d'Accès à Internet (FAI) ont l'obligation d'enregistrer les adresse IP des serveurs de sites webs auxquels se connecte un utilisateur[1]. Ils n'ont pas le droit d'enregistrer les adresses URL consultées, ni le contenu des échanges, mais savent que tel utilisateur a demandé a avoir accès a tel site internet. Et cela donne déjà beaucoup d'informations aux enquêteurices qui se pencheraient sur ces données : ça permet de dresser assez bien la personnalité de la personne espionnée. Si elleux ne peuvent pas savoir quel texte tu es allé.e lire sur The Anarchist Library, elleux savent que tu consultes régulièrement ce site, et ça peut leur suffire.

Prenons un exemple. Un texte de revendication d'action est publié sur un blog de Blogspot. Blogspot a enregistré l'adresse IP de l'utilisateur ayant publié ce texte. Blogspot la fournit à la police après avoir reçu une réquisition. En demandant au FAI quel était l'utilisateur.ice de l'adresse IP donnée au moment de la publication, les policier.es peuvent obtenir l'identité de l'auteur du texte.

L'utilisation de Tor Browser permet assez efficacement d'anonymiser sa navigation internet. On ne s'étendra pas en explications techniques, mais plutôt que de mettre directement en relation un téléphone ou un ordinateur avec un serveur, Tor Browser fait transiter cette demande par 3 serveurs parmi les miliers de serveurs du réseau Tor. Ainsi, le serveur demandé ne connaît pas l'adresse IP de l'utilisateur, mais l'adresse IP du troisième serveur Tor.

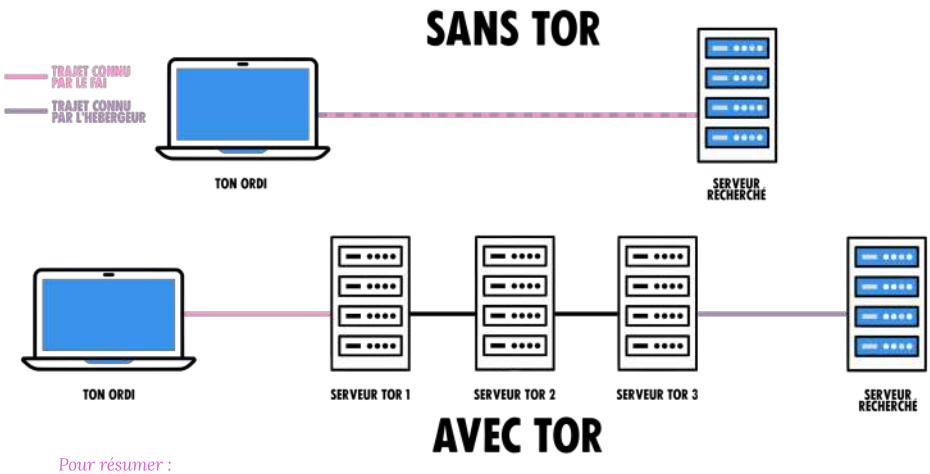
Dans notre exemple, le serveur de blogspot n'associerait pas à la publication de l'article l'adresse IP de son auteur, mais celle du 3e serveur Tor. La police, après avoir obtenu cette adresse IP en envoyant une réquisition à Blogspot, découvrirait que celle-ci est l'IP d'un des milliers de serveurs et du réseau Tor, et ne pourrait pas aller plus loin.

En utilisant Tor, le FAI ne peut connaître que l'adresse IP du premier serveur Tor que nous consultons. Il ne sait pas quel site nous demandons en réalité. Un.e enquêteurice qui lirait ces données saurait que nous nous connectons à Tor, ce qu'il peut considérer comme étant un geste suspect, mais n'en saurait pas plus. Tor rend caduque l'exploitation des données de connexion des FAI et des hébergeurs.

Tor a cependant ses limites, et certains services de renseignements laissent entendre qu'ils ont les capacités techniques de désanonymiser des utilisations de Tor de manière extrêmement ciblée, et donc ici de retrouver qui est l'auteur.ice de l'article même si celui-ci a utilisé Tor. Mais cette désanonymisation ne se fait vraiment pas facilement, et demande probablement des moyens importants. Le risque de désanonymisation est donc très faible.

En 2021, dans une enquête de police sur la lutte contre la gentrification du quartier parisien de Sainte-Marthe, la police a envoyé des réquisitions demandant à Protonmail et à Instagram de donner toutes les informations permettant d'identifier les utilisateurs d'une adresse mail Protonmail et d'un compte Instagram sur lesquels iels enquêtaient.

1. Sur les obligations d'enregistrement pour les FAI et les hébergeurs : https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000044228890



Pour résumer :
- Sans Tor, le FAI relie l'identité et l'adresse IP de l'utilisateur, et connaît les adresse IP des serveurs de sites internets recherchés. L'hébergeur connaît l'adresse IP de l'utilisateur ;
- Avec Tor, le FAI relie l'identité et l'adresse IP de l'utilisateur, il connaît l'adresse IP du premier serveur Tor utilisé, il peut donc savoir que l'utilisateur utilise Tor. L'hébergeur connaît lui l'adresse IP du troisième serveur Tor

Protonmail a fourni l'adresse IP avec laquelle l'adresse mail a été créée, et la police n'a pas tenté de relier cette adresse IP à une identité[1]. Si lea créateurice de l'adresse mail avait créé cette adresse sans utiliser Tor, et que les policiers avaient demandé l'identification de l'adresse, cette dernière aurait réussi. L'utilisation des données conservées par les hébergeurs et les FAI n'est pas une pratique rare, et Tor – qui a ses limites – permet de l'empêcher.

Depuis 2015, il existe des dispositifs de renseignements, les « boîtes noires ». Laissons le journal bourgeois Le Monde nous expliquer : « *La loi prévoit qu'un algorithme examine des métadonnées (horaire, origine, destination d'un message, mais pas son contenu), puisées sur les réseaux de communication pour les trier et déterminer si des éléments doivent retenir l'attention* [c'est-à-dire s'ils indiquent la participation ou la préparation d'un truc terroriste] »[2]. Ces données peuvent ensuite être, sur demande, désanonymisées, c'est-à-dire que si un profil « *retient l'attention* », les policiers ont le droit de désanonymiser le trafic, pour trouver l'identité de la personne. Cette technique est pour l'instant légalement limitée à l'identification de la menace terroriste, mais on sait que les services de renseignement peuvent avoir une acception du terme à géométrie variable. Tor empêche aussi ce type d'enquête, puisqu'il empêche que la désanonymisation se fasse.

L'arrêt de la cour de cassation dont on a parlé plus haut, sur le stockage des données de connexion, concerne aussi la conservation des données par les FAI et les hébergeurs, et limite donc théoriquement leur utilisation. L'avenir nous dira si ces limitations se traduiront dans les faits.

1. https://paris-luttes.info/recit-policier-de-sainte-marthe-15258?lang=fr
2. https://www.lemonde.fr/pixels/article/2017/11/14/les-boites-noires-de-la-loi-sur-le-renseignement-sont-desormais-actives_5214596_4408996.html

Comme pour les téléphones, les policier.es peuvent exploiter les données contenues sur le disque dur d'un ordinateur. Et c'est même beaucoup plus simple pour elleux. Les ordis qui tournent sous Windows et la plupart des systèmes d'exploitation Linux ne sont pas chiffrés, leurs données sont donc très facilement lisibles. Ce n'est pas le cas des ordinateurs tournant sur MacOs, qui sont par défauts chiffrés. Leur exploitation pose plus de difficultés à la police, mais elle n'est pas impossible – elle demande de gros moyens, et ne sera pas utilisée dans n'importe quelle affaire. Les policier.es peuvent donc avoir accès à tous les documents stockés sur le disque dur, notamment l'historique internet, qui est sauvegardé pour une certaine durée par les navigateurs. Iels pourront donc y trouver les photos que vous avez faites des voitures de keufs dont vous revendiquez l'incendie, les textes ultra déters d'appels à action que vous écrivez, iels pourront voir que vous consultez souvent le site hautement subversif paris-luttes.info, ...

Tails, c'est un système d'exploitation créé spécialement pour la sécurité numérique. Donc forcément, il est un minimum utile. C'est un système *live*, c'est-à-dire qu'il est installé sur une clé USB, un CD, une carte SD, mais pas sur un disque dur interne. Tails ne laisse, après qu'on l'ait éteint, aucune trace sur les ordinateurs sur lesquels il est utilisé. Aucune donnée n'est enregistrée sur le disque dur de l'ordinateur. Si toute mon activité militante passe par Tails, l'exploitation du disque dur de l'ordinateur ne donnera jamais rien.

Par défaut, Tails permet de n'utiliser que Tor Browser. Par défaut aussi, Tails masque l'adresse Mac de l'ordinateur utilisé (l'adresse Mac, c'est le numéro de série de la partie de l'ordinateur qui permet de se connecter à internet, la carte réseau), adresse qui est parfois utilisé pour espionner l'activité en ligne de certains utilisateurs, et de les identifier.

Si j'ai besoin de sauvegarder des données sur Tails, Tails les chiffre. Le document de traitement de texte sur lequel vous préparez votre texte de revendication pour l'incendie des voitures de keufs sera illisible par les policiers. La vidéo de riot porn que vous êtes en train de monter sera, de même, illisible. Aucune trace non plus de votre historique internet. Rappelons quand-même que c'est un délit – puni de 3 ans de prison et de 370 000 euros d'amende – de refuser de donner la phrase de passe qui vous permet d'accéder aux fichiers enregistré sur votre clé Tails. Mais ces peines ne sont jamais appliquées telles quelles, et il ne fait aucun doute que se retrouver accusé.e de ce délit est toujours avantageux plutôt que faire tomber toutes nos données entre les mains de la police.

Les services de renseignement, comme ils en ont le droit pour les smartphones, peuvent installer sur les ordinateurs des logiciels espions qui permettent d'accéder au contenu de l'écran, aux frappes clavier, à la localisation, aux caméras et aux micros du support numérique. Avec Tails, leur mise est place est fortement limitée, nécessite d'utiliser des techniques plus complexes que pour installer un logiciel espion sur Windows 10. Tails est en tout cas une première limite, même si elle n'a rien de sûr.

En conclusion, utiliser Tails limite, ou en tous cas complexifie l'utilisation de logiciels espions, protège de nombreuses attaques possibles, permet de protéger les données qu'on veut sécuriser et ne laisse aucune trace sur les disques durs des ordinateurs utilisés.

Tout dépend vraiment de ce qu'on a à cacher. C'est pas la même chose de préparer des collages d'affiches ou des attaques à la bombe. À chaque groupe d'adapter sa sécurité à ce qu'il fait. Mais en général, on peut se dire que c'est toujours une mauvaise idée d'avoir son téléphone sur soi en manif ou en action. On peut se dire aussi qu'il ne faut jamais échanger d'informations compromettantes par SMS ou par appel téléphonique. Plus globalement, on ne peut que conseiller de ne pas se servir d'outils numériques pour préparer des choses compromettantes, sauf quand on en a vraiment besoin.

Il faut aussi se souvenir que les keufs utilisent toujours leurs bonnes vieilles méthodes, d'enquêtes, d'espionnage et de renseignement, que c'est plus simple pour elleux de faire des contrôles d'identité à toustes les participant.es d'un rassemblement plutôt que d'identifier toutes les personnes ayant borné sur les lieux de ce rassemblement, et que c'est plus simple pour elleux de « filer », de suivre, quelqu'un.e que d'installer un logiciel espion récupérant la géolocalisation d'un téléphone.

QUELQUES RESSOURCES…

Sur le téléphone en garde-à-vue :

- *Garde à vue : ne dites rien, votre téléphone parlera pour vous* : https://www.dalloz-actualite.fr/node/garde-vue-ne-dites-rien-votre-telephone-parlera-pour-vous#.YveWJN_LeuI
- Sur les UFED : https://www.streetpress.com/sujet/1579520319-police-gendarmerie-un-logiciel-pour-fouiller-portables
- le site web de Cellebrite : https://cellebrite.com/fr/cellebrite-ufed-fr

Sur les fadettes et l'usage de la téléphonie mobile :

- *Investigations & téléphonie mobile. Le guide à l'usage des avocat.es* : https://attaque.noblogs.org/files/2021/05/Investigations-telephonie-mobile-up.pdf
- *Analyse d'un dossier antiterroriste* : https://infokiosques.net/IMG/pdf/analyse_d_un_dossier_d_instruction_antiterroriste.pdf

Sur Tails et Tor :

- *TuTORiel Tails*, un tuto très précis sur l'utilisation de Tails : https://infokiosques.net/spip.php?article1726
- des explications pas claires mais précises sur le fonctionnement de Tor : https://fr.wikipedia.org/wiki/Tor_(r%C3%A9seau)

En général, sur la sécurité numérique, et le renseignement :

- Le *guide d'autodéfense numérique*, la bible des geeks anarchisant.es (il y a vraiment tout dedans) : https://guide.boum.org/
- Le *Guide de survie en protection numérique à l'usage des militant·es* : https://infokiosques.net/spip.php?article1849
- Les pages *Sécurité* de riseup.net : https://riseup.net/fr/security

***Des brochures d'antirep* :**

- Le *petit manuel de défense collective : de la rue au tribunal* de la défense collective paris-banlieues : https://defensecollectiveparisbanlieues.noblogs.org/brochure-de-a-a-z/