Notes

[1] Bien avant d'imaginer la « sécurité globale », l'État (gouvernement « gauche plurielle » mené à l'époque par le socialo Jospin) avait prévu d'intégrer la sécurité à nos quotidiens. La loi sur la sécurité quotidienne (LSQ) du 15 novembre 2001, préparée bien avant les attentats, s'alourdit d'un paquet de mesures antiterroristes (dont le croisement de divers fichiers policiers, la rétention obligatoire des données internet et téléphoniques, cet article sur les messages chiffrés, etc.). La LSQ va notamment créer l'Institut national de police scientifique, et rendre passible de prison le fait de refuser un prélèvement ADN, étendant par ailleurs la liste des infractions passibles d'une inscription au FNAEG au-delà des seuls faits de délinquance sexuelle.

[2] Sous IOS, les derniers iPhone (7 ou 8 ? on a un doute) sont chiffrés par défaut, c'est-à-dire que le disque dur est protégé par le code ou mot de passe de déverrouillage. Sous Android, il faut effectuer l'opération à la main (option sécurité > chiffrer).

Liens :

a : https://paris-luttes.info/code-pin-en-garde-a-vue-decryptage-10696
b : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000036756797/
c : https://www.courdecassation.fr/jurisprudence_2/chambre_criminelle_578/1804_13_45671.html
d : https://www.dalloz-actualite.fr/flash/code-d-acces-d-un-telephone-une-convention-de-dechiffrement
e : https://www.courdecassation.fr/jurisprudence_2/chambre_criminelle_578/90_12_46258.html
f : https://guide.boum.org/
g : https://zadducarnet.org/index.php/2021/01/10/guide-de-survie/
h : https://www.service-public.fr/particuliers/vosdroits/R33420
i : http://paris-luttes.info/les-flics-d-iles-de-france-ont-12984
j : http://paris-luttes.info/point-secu-le-kiosk-arme-ultime-de-14182
k : https://www.lameute.info/posts/signal-balance-un-incroyable-scud-aux-polices-du-monde-entier
l : https://paris-luttes.info/sortez-couvert-e-s-7928

Du nouveau sur l'obligation de donner son code de téléphone en garde-à-vue :

comment éviter le traquenard

Publié le 17 mai 2021 sur paris-luttes.info

On avait dénoncé un coup de bluff[a], mais ils en ont fait un traquenard. Que faire lorsque les flics, en garde à vue, exigent d'obtenir votre code pour accéder aux données de votre téléphone ?

Pour les conseils pratiques, voir #en-bas

Pour mieux comprendre pourquoi les keufs se jettent sur votre appareil, disons que tout semble venir du principe de garder le silence. C'est un droit, beaucoup ont appris à l'exercer (tant bien que mal), mais flics et juges en ont marre de se trouver face à des gens inflexibles qui répètent « je n'ai rien à déclarer ». Le droit de garder le silence répond pourtant au droit de ne pas s'auto-incriminer (reconnu à l'article 6 de la Convention européenne des droits de l'homme), qui lui-même découle de la présomption d'innocence : c'est à l'accusation, pas à l'accusé-e, de démontrer qu'un délit ou un crime a bien été commis !

Entre les mains des bleus, notre téléphone portable peut rapidement devenir la boite de Pandore de l'incrimination. Bien entendu, un téléphone mobile basique est beaucoup moins intéressant à exploiter qu'un smartphone doté d'un accès internet. Mais on y trouve quand même votre carnet d'adresse, le journal des appels et les SMS échangés. On peut le protéger avec un code PIN, mais s'il est saisi alors qu'il est encore allumé, tout apparaît en clair.

Mais franchement, ce qui intéresse les flics c'est de fouiller dans le petit ordinateur mobile qu'on appelle un smartphone. On le protège par un code PIN (carte SIM) mais surtout avec un code ou mot de passe de déverrouillage. C'est dans cette machine que se cache nos vies, intimes et politiques, débordantes d'infos sur nos militantismes et nos relations personnelles. Avant que ces infos puissent servir à nous incriminer, leur objectif principal est de nous rendre encore plus vulnérables pendant l'interrogatoire... Tu ne veux rien dire ? Et bien le keuf va te faire réagir en matant dans ton tel ! Ainsi, on se retrouve vite qualifié.e de « militant.e pro-kurde » pour avoir communiqué sur une conférence sur le Rojava, « d'activiste féministe » pour avoir parlé à un.e pote de la manif du 8 mars, voire même de « casseur.se » pour le simple fait d'être membre d'un groupe Telegram de Gilets jaunes ou pris en photo devant un tag « ACAB ». Notre petit écran mobile se transforme alors en notre meilleur ennemi, livrant aux flics des moyens de pression pour nous intimider, voire même des infos susceptibles de faire aussi poursuivre nos proches et nos contacts.

Le traquenard est donc le suivant : « *soit tu donnes ton code, soit on te confisque ton téléphone, on le met sous scellés et tu peux l'oublier !* » C'est un vrai chantage. Et les juges enfoncent le clou : il est arrivé que des personnes soient relaxées pour un délit mineur mais que leur téléphone reste sous scellé, dans le coffre du comico ou du tribunal pour avoir refusé de coopérer en ne donnant pas son code ! Relaxé, mais puni d'avoir usé de son droit au silence ! Exactement

- Téléphone non chiffré avec un code de déverrouillage : les données aspirées seront sans doute exploitables en clair ; refuser de leur donner le code les empêche juste de les exploiter sur le champ ;
- Téléphone chiffré, avec code de déverrouillage, mais encore sous tension (non éteint) au moment de l'aspiration : certaines données pourront apparaître en clair.
- Téléphone chiffré mais éteint pendant l'exploitation : scénario le plus sûr, les données stockées sur le disque principal, devraient rester illisibles sans le code ou mot de passe ; d'où l'intérêt d'éteindre sa machine dès qu'on est entre les mains des flics.

En sachant que :

- il existe des méthodes, selon les modèles, pour bloquer l'accès aux données via le port USB...
- Attention aux cartes SD externes, qui peuvent contenir photos, vidéos ou autres trucs très personnels : parfois il faut les chiffrer à part, et parfois on ne peut pas du tout les chiffrer !

Enfin, une bonne nouvelle à annoncer face au déferlement répressif. Signal, cette application libre, open-source et gratuite permettant d'échanger des messages et des appels chiffrés de bout en bout, a récemment annoncé avoir réussi à saboter le logiciel Cellebrite qui fait fonctionner ce « kiosk ». Il suffira de télécharger la nouvelle version de Signal, qui comportera des fichiers pouvant mettre à mal Cellebrite. Pour plus d'infos sur comment Signal a balancé un incroyable scud aux polices du monde entier, c'est par ici[k] !

Legal Team Paris

—

Rappel de la ligne (ouverte par intermittence) : 07.52.95.71.11
Hors urgence, écrire à stoprepression(AT)riseup.net
Conseils et stratégies : brochure « Sortez couvert-e-s »[l]
Pour alimenter la caisse collective : https://www.helloasso.com/associations/collectives-solidarites

- **Maintiens ton droit au silence** en garde-à-vue, et **refuse de donner ton code** ! Si tu es poursuivi.e pour ce délit, tu pourras te défendre (et être défendu.e par ton avocat.e) devant le juge.
- Mais surtout : **laisse ton tel chez toi !** Il est mille fois plus simple de prendre un *burner* (un tel basique) le temps d'une manif ou d'une action, ou tout simplement de s'organiser en amont avec tes potes pour bouger sans portable, pour éviter que les flics mettent la main dessus.

Peut-on récupérer son smartphone confisqué ?

Si on a refusé de coopérer en gardant sa langue et son code de déverrouillage, en cas de saisie du portable, après la GAV ou le jugement, il existe un formulaire[h] « *restitution d'un bien placé sous main de justice* ». Remplis-le et demande à ton avocat.e de faire un courrier / mail au procureur afin d'en réclamer la restitution — sans aucune garantie de succès...

A propos du chiffrement

Si tu hésites encore à chiffrer ton smartphone [2], prends un moment pour lire cet article :

> **Les flics ont maintenant une machine pour aspirer l'ensemble des données de votre mobile**[i]
>
> Suite à un reportage de Reporterre et un article de Checknews, on a maintenant la confirmation que les commissariats d'Île-de-France vont s'équiper d'une centaine de nouvelles machines capables d'aspirer l'ensemble des (...)

ou celui-ci, plus fouillé mais beaucoup plus technique :

> **Point sécu : le « kiosk », arme ultime de la police ?**[j]
>
> La nouvelle a fait grand bruit : la police va se doter sous peu de boîtiers qui seraient capables de rentrer dans virtuellement n'importe quel smartphone, aussi protégé soit-il. C'est en fait pas si simple que ça ! Texte (...)

En résumé, le « kiosk » est une petite boite électronique scélérate qui, connectée via le port USB, peut aspirer toutes les données du disque principal en quelques minutes et qui seront, ensuite, exploitées tranquillou par les keufs. A terme, tous les comicos seront équipés de cette boite magique. Mais cette méthode de flicage n'est pas infaillible ! Quatre principaux scénarios possibles :

- Téléphone non chiffré sans code de déverrouillage : tout apparaît en clair, pas besoin de la petite boite magique...

comme le refus de signalétique ou d'ADN, ces délits « autonomes » sont autant de moyens de pression sur les personnes interpellées.

Les hauts magistrats nous l'ont fait à l'envers

Sur quelle base juridique la justice nous fait ce chantage dégueulasse ? L'article 434-15-2 du Code pénal :

> « *Est puni de trois ans d'emprisonnement et de 270 000 € d'amende le fait, pour quiconque ayant connaissance de la* ***convention secrète de déchiffrement d'un moyen de cryptologie*** *susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités [...].*
>
> *Si le refus est opposé alors que la remise ou la mise en œuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 450 000 € d'amende.* »

Ce texte existe depuis... 2001, et se trouve dans une loi adoptée "en urgence" juste après les attentats du 11 septembre. [1] Au départ, ce délit visait à lutter contre les « *actes de terrorisme ou de grande criminalité* » . Les peines prévues ont été de nouveau aggravées par la loi anti-terroriste du 3 juin 2016. Il est question de cryptologie : l'art de protéger un message par un système de chiffrement. Le deal était le suivant : chacun-e possède le droit de crypter ses messages privés, mais en échange la justice exigeait de pouvoir obtenir la clé de décryptage si elle estimait que des messages protégés auraient pu être "*utilisés pour préparer, faciliter ou commettre un crime ou un délit*".

Alors comment se fait-il que ce même article puisse servir à intimider une personne en garde-à-vue afin qu'iel coopère en donnant *full access* à son téléphone ? Car cela entre clairement en conflit avec le droit à ne pas s'auto-accuser !

En gros, les haut magistrats - Conseil constitutionnel et Cour de cassation — nous l'ont fait à l'envers en plusieurs étapes.

- **Concernant le droit de ne pas s'auto-incriminer**. C'est le Conseil constitutionnel qui a dégainé le premier (décision QPC du 30 mars 2018[b]). Selon Laurent Fabius (président du conseil constit') et ses potes, cet article 434-15-2 ne porte pas atteinte au droit de ne pas s'auto-incriminer car les données contenues dans le téléphone "*existent indépendamment de la volonté de la personne suspectée et peuvent être obtenues par des moyens techniques*". Interprétation très tendancieuse : on ne participe pas à notre propre incrimination en livrant aux flics des infos personnelles... qui seront très certainement utilisées pour nous incriminer !

- **A propos de "convention secrète d'un moyen de cryptologie"**. Un code de déverrouillage de téléphone est-il un moyen de chiffrement ? La Chambre criminelle de la Cour de cass a répondu oui sans nuance (arrêt du 13 octobre 2020[c]). Elle contredit un précédent jugement de la Cour d'appel de Paris (16 avril 2019), pour qui « *un code de déverrouillage d'un téléphone portable d'usage courant (…) ne permet pas de déchiffrer des données ou messages cryptés et, en ce sens, ne constitue pas une convention secrète d'un moyen de cryptologie* » et a donc condamné l'auteur du pourvoi pour avoir « *refusé de répondre aux enquêteurs et de communiquer les codes de déverrouillage de ses téléphones* ». Pour une lecture moins complexe de cet arrêt, c'est ici[d].
- **A propos de "l'autorité judiciaire".** L'article 434-15-2 énonce clairement que l'obligation est de "*remettre ladite convention aux autorités judiciaires*". En GAV on a affaire à un OPJ (officier de police judiciaire), en aucun cas à un magistrat qui relève de "*l'autorité judiciaire*" (juge d'instruction ou procureur). Pourtant la Cour de cass (dans ce même arrêt) prend ses aises en estimant : "*la réquisition délivrée par un officier de police judiciaire (...), sous le contrôle de l'autorité judiciaire, entre dans les prévisions de l'article 434-15-2 du code pénal*". Seule condition mise en avant par la cour : l'OPJ doit énoncer "*un avertissement que le refus d'y déférer est susceptible de constituer une infraction pénale*". La Cour de cass ne parle jamais de *proportionnalité* entre la violation de la vie privée (accéder à l'intégralité des données) et le délit présumé !
- **"Assimilable à une perquisition"**. Dans un arrêt plus récent (12 janvier 2021[e]), la même Chambre criminelle estime que, lors d'une audition en GAV, même sans la présence d'un.e avocat.e, exiger d'exploiter le téléphone sur le champ est "*assimilable à une perquisition*", opération qui peut en effet se dérouler sans avocat-e. Mais lors d'une perquisition, des garanties existent : la personne visée doit être présent.e, ou bien désigner deux témoins "neutres" (hors effectifs de police), et elle peut assister aux saisies effectuées. Rien de tout ça en GAV, et rien n'oblige les flics à exploiter le téléphone en présence du suspect. La cour de cassation s'en balance : tout est réglo !

Après cette pénible démonstration, il faut donc se rendre à l'évidence : les juges ont validé ce chantage policier en détournant ce délit. Les flics s'en réjouissent, et en profitent pour menacer de confisquer votre petit appareil électronique si vous ne coopérez pas.

Quelle attitude adopter ?

Pourtant, tout n'est pas pas perdu. Bien que les keufs s'en donnent à coeur joie pour confisquer nos portables, des moyens de défense existent dans le cas où on serait poursuivi pour refus d'ouvrir son tel devant un juge.

Rappel des conditions demandées pour faire jouer l'article 434-15-2 du Code pénal :

- Pour établir que la demande **émane d'une autorité judiciaire**, il faut donc (comme vu plus haut) qu'une réquisition écrite soit fournie par un magistrat, bien que la Cour de cass a largement facilité cette formalité.
- **il faut avoir été prévenu** (cf "*l'avertissement*") **que refuser de donner son code constitue un délit** : cela doit apparaître sur un des PV ; en absence de PV, ça pourrait motiver une demande de nullité lors du procès, mais sans garantie de succès....
- il faut **prouver que cette demande ait un intérêt pour l'enquête**, avec l'existence de données sur le portable qui auraient été « *utilisées pour préparer, faciliter ou commettre un crime ou un délit* ». Si rien ne permet de soutenir que le téléphone aurait servi pour de tels faits, tu as une bonne raison de ne pas fournir le code de déverrouillage.
    - Par exemple, arrêté.e pour outrage ou rébellion, il parait très peu probable que les données se trouvant dans un portable aient servi à préparer ou faciliter ces délits : ça peut tout à fait justifier, devant les juges, le refus de donner ton code.
    - En revanche, ce sale délit de "*groupement en vue de*", très souvent motivé pour justifier des arrestations massives en manifs ou lors d'agitations émeutières dans les quartiers populaires, est un motif idéal pour que les keufs fouillent dans les portables...

Ces conditions ne sont souvent pas remplies en garde à vue, quoiqu'en disent les keufs. Bien sur, il semble compliqué, retenu.e et entravé.e, de pouvoir exiger d'eux qu'ils justifient des conditions de mise en œuvre de ce délit. On imagine mal qu'on puisse, après 48h de conditions difficiles et entouré.e de flicaille, sommer à l'OPJ de nous expliquer pourquoi la fouille de notre téléphone aurait un intérêt pour l'enquête.

Le plus simple reste à **garder le silence**, ne pas lâcher ton code, et ce même lorsque les flics t'expliqueront que tu commets un délit. Il vaut mieux **attendre de voir si le procureur décide de te poursuivre,** car il y a de très nombreux cas de personnes qui ressortent avec leur portable et sans n'avoir rien lâché. Si des poursuites sont engagées, tu pourras te défendre (et être défendu.e par ton avocat.e) devant le juge, en faisant valoir ces arguments. Bien que le Code pénal réprime ce délit de trois ans d'emprisonnement et de 270.000 € d'amende, les condamnations, lorsqu'elles sont prononcées malgré tout par le juge, s'élèvent rarement à plus que des petites amendes.

Quelques conseils

- **Protège ton portable !** Des guides d'auto-défense numériques existent ici[f] ou là[g], mais pour faire court : il vaut mieux que ton portable ait un code de verrouillage, que ta carte SIM ait un code PIN, et que les données de ton téléphone soient chiffrées. Ces manœuvres sont simples à effectuer, et permettent de ne pas accueillir les fouines policières dans ton cocon numérique