https://ricochets.cc/L-Etat-criminalise-la-securite-informatique-soyons-toustes-clandestin-es.html

L'Etat criminalise la sécurité informatique : soyons toustes Â« clandestin.es Â» ?!

- Les Articles -

Date de mise en ligne : samedi 10 juin 2023

Face à cette criminalisation accrue de simples outils numériques sécurisés, deux options :

1. ne quasi plus utiliser les outils numériques en général
2. qu'un maximum de monde utilise couramment des outils numériques cryptés et sécurisés (VPN, bloqueurs de pubs et de cookies, Signal, ProtonMail, Tor, Tails, F-Droid, chiffrement de téléphone et de disque dur, etc.)

Affaire du 8 décembre : le chiffrement des communications assimilé à un comportement terroriste

Cet article a été rédigé sur la base d'informations relatives à l'affaire dite du "8 décembre" dans laquelle 7 personnes ont été mises en examen pour « association de malfaiteurs terroristes » en décembre 2020. Leur procès est prévu pour octobre 2023. Ce sera le premier procès antiterroriste visant « l'ultragauche » depuis le fiasco de l'affaire Tarnac.

L'accusation de terrorisme est rejetée avec force par les inculpé·es. Ces dernier·es dénoncent un procès politique, une instruction à charge et une absence de preuves. Ils et elles pointent en particulier des propos decontextualisés et l'utilisation à charge de faits anodins (pratiques sportives, numériques, lectures et musiques écoutées...). De son côté la police reconnaît qu'à la fin de l'instruction - et dix mois de surveillance intensive - aucun « projet précis » n'a été identifié.

L'État vient d'être condamné pour le maintien à l'isolement du principal inculpé pendant 16 mois et dont il n'a été libéré qu'après une grève de la faim de 37 jours. Une seconde plainte, en attente de jugement, a été déposée contre les fouilles à nu illégales et répétées qu'une inculpée a subies en détention provisoire.

De nombreuses personnalités, médias et collectifs leur ont apporté leur soutien.

C'est dans ce contexte que nous avons été alerté du fait que les pratiques numériques des inculpé·es - au premier rang desquelles l'utilisation de messageries chiffrées grand public - sont instrumentalisées comme « preuves » d'une soi-disant « clandestinité » venant révéler l'existence d'un projet terroriste inconnu.

Nous avons choisi de le dénoncer.

« Tous les membres contactés adoptaient un comportement clandestin, avec une sécurité accrue des moyens de communications (applications cryptées, système d'exploitation Tails, protocole TOR permettant de naviguer de manière anonyme sur internet et wifi public). »

DGSI

« L'ensemble des membres de ce groupe se montraient particulièrement méfiants, ne communiquaient entre eux que par des applications cryptées, en particulier Signal, et procédaient au cryptage de leurs supports informatiques [...]. »
Juge d'instruction

Ces deux phrases sont emblématiques de l'attaque menée contre les combats historiques de La Quadrature du Net dans l'affaire du 8 décembre que sont le droit au chiffrement7 des communications8, la lutte contre l'exploitation des données personnelles par les GAFAM9, le droit à l'intimité et la vie privée ainsi que la diffusion et l'appropriation des connaissances en informatique.

Mêlant fantasmes, mauvaise foi et incompétence technique, les éléments qui nous ont été communiqués révèlent qu'un récit policier est construit autour des (bonnes) pratiques numériques des inculpé·es à des fins de mise en scène d'un « groupuscule clandestin », « conspiratif » et donc... terroriste.

Voici quelques-unes des habitudes numériques qui sont, dans cette affaire, instrumentalisées comme autant de « preuves » de l'existence d'un projet criminel :

- l'utilisation d'applications comme Signal, WhatsApp, Wire, Silence ou ProtonMail pour chiffrer ses

communications ;
- le recours à des outils permettant de protéger sa vie privée sur Internet comme un VPN, Tor ou Tails ;
- le fait de se protéger contre l'exploitation de nos données personnelles par les GAFAM via des services comme /e/OS, LineageOS, F-Droid
- le chiffrement de supports numériques
- l'organisation et la participation à des sessions de formation à l'hygiène numérique
- la simple détention de documentation technique.

Alors que le numérique a démultiplié les capacités de surveillance étatiques, nous dénonçons le fait que les technologies qui permettent à chacun·e de rétablir un équilibre politique plus que jamais fragilisé soient associées à un comportement criminel à des fins de scénarisation policière.
(...)
Durant la phase d'enquête, l'amalgame entre chiffrement et clandestinité est mobilisé pour justifier le déploiement de moyens de surveillance hautement intrusifs comme la sonorisation de lieux privés. La DGSI les juge nécessaires pour surveiller des « individus méfiants à l'égard du téléphone » qui « utilisent des applications cryptées pour communiquer ».
(...)
« Pourquoi utilisez-vous ce genre d'applications de cryptage et d'anonymisation sur internet ? ». Le lien supposé entre chiffrement et criminalité est clair : « Avez-vous fait des choses illicites par le passé qui nécessitaient d'utiliser ces chiffrements et protections ? », « Cherchez-vous à dissimuler vos activités ou avoir une meilleure sécurité ? ». Au total, on dénombre plus de 150 questions liées aux pratiques numériques.
(...)
Le PNAT consacrera un chapitre entier aux « moyens sécurisés de communication et de navigation » au sein d'une partie intitulée... « Les actions conspiratives ». Sur plus de quatre pages le PNAT fait le bilan des « preuves » de l'utilisation par les inculpé·es de messageries chiffrées et autres mesures de protection de la vie privée. L'application Signal est particulièrement visée.
Citons simplement cette phrase : « Les protagonistes du dossier se caractérisaient tous par leur culte du secret et l'obsession d'une discrétion tant dans leurs échanges, que dans leurs navigations sur internet. L'application cryptée signal était utilisée par l'ensemble des mis en examen, dont certains communiquaient exclusivement [surligné dans le texte] par ce biais. ».
(...)

Au-delà du chiffrement des communications, ce sont aussi les connaissances en informatique qui sont incriminées dans cette affaire

Au-delà du chiffrement des communications, ce sont aussi les connaissances en informatique qui sont incriminées dans cette affaire : elles sont systématiquement assimilées à un facteur de « dangerosité ».
La note de la DGSI, évoquée ci-dessus, précise ainsi que parmi les « profils » des membres du groupe disposant des « compétences nécessaires à la conduite d'actions violentes » se trouve une personne qui posséderait de « solides compétences en informatique et en communications cryptées ». Cette personne et ses proches seront, après son arrestation, longuement interrogé·es à ce sujet.
La simple détention de documentation informatique est elle aussi retenue comme un élément à charge.
Parmi les documents saisis suite aux arrestations, et longuement commentés, se trouvent des notes manuscrites relatives à l'installation d'un système d'exploitation grand public pour mobile dégooglisé (/e/OS) et mentionnant diverses applications de protection de la vie privée (GrapheneOS, LineageOS, Signal, Silence, Jitsi, OnionShare, F-Droid, Tor, RiseupVPN, Orbot, uBlock Origin...).
(...)
L'incrimination des compétences informatiques se double d'une attaque sur la transmission de ces dernières. Une partie entière du réquisitoire du PNAT, intitulée « La formation aux moyens de communication et de navigation sécurisée », s'attache à criminaliser les formations à l'hygiène numérique, aussi appelées « Chiffrofêtes » ou « Cryptoparties ».

Ces pratiques collectives et répandues - que La Quadrature a souvent organisées ou relayées - contribuent à la diffusion des connaissances sur les enjeux de vie privée, de sécurisation des données personnelles, des logiciels libres et servent à la réappropriation de savoirs informatiques par toutes et tous.

Qu'est-il donc reproché à ce sujet dans cette affaire ? Un atelier de présentation de l'outil Tails, système d'exploitation grand public prisé des journalistes et des défenseurs·ses des libertés publiques. Pour le PNAT c'est lors de cette formation que « X les a dotés de logiciels sécurisés et les a initiés à l'utilisation de moyens de communication et de navigation internet cryptés, afin de leur garantir l'anonymat et l'impunité ». Le lien fait entre droit à la vie privée et impunité, corollaire du fantasme policier d'une transparence totale des citoyen·nes, a le mérite d'être clair.

(...)

Pire, ce dernier ira jusqu'à retenir cette formation comme un des « faits matériels » caractérisant « la participation à un groupement formé [...] en vue de la préparation d'actes de terrorisme », tant pour la personne l'ayant organisé - « en les formant aux moyens de communication et de navigation internet sécurisés » - que pour celles et ceux l'ayant suivi - « en suivant des formations de communication et de navigation internet sécurisés ».

(...)

Une réponse inspirera particulièrement le PNAT qui écrira : « Il avait convaincu sa mère d'utiliser des modes de communication non interceptables comme l'application Signal. »

(...)

Même la relation à la technologie et en particulier aux GAFAM - contre lesquels nous sommes mobilisés depuis de nombreuses années - est considérée comme un signe de radicalisation. Parmi les questions posées aux mis·es en examen, on peut lire : « Etes-vous anti GAFA ? », « Que pensez-vous des GAFA ? » ou encore « Eprouvez-vous une certaine réserve vis-à-vis des technologies de communication ? ».

(...)

Comment est-il possible qu'un tel discours ait pu trouver sa place dans un dossier antiterroriste ? Et ce sans qu'aucun des magistrat·es impliqué·es, en premier lieu le juge d'instruction et les juges des libertés et de la détention, ne rappelle que ces pratiques sont parfaitement légales et nécessaires à l'exercice de nos droits fondamentaux ? Les différentes approximations et erreurs dans les analyses techniques laissent penser que le manque de compétences en informatique a sûrement facilité l'adhésion générale à ce récit.

(...)

Que dire enfin des remarques récurrentes du juge d'instruction et du PNAT quant au fait que les inculpé·es chiffrent leurs supports numériques et utilisent la messagerie Signal ?

Savent-ils que la quasi-totalité des ordinateurs et téléphones vendus aujourd'hui sont chiffrés par défaut ? Les leurs aussi donc - sans quoi cela constituerait d'ailleurs une violation du règlement européen sur la protection des données personnelles.

Quant à Signal, accuseraient-ils de clandestinité la Commission Européenne qui a, en 2020, recommandé son utilisation à son personnel ? Et rangeraient-ils du côté des terroristes le rapporteur des nations Unies qui rappelait en 2015 l'importance du chiffrement pour les droits fondamentaux ? Voire l'ANSSI et la CNIL qui, en plus de recommander le chiffrement des supports numériques osent même... mettre en ligne de la documentation technique pour le faire ?

(...)

La mise en avant du chiffrement offre un dernier avantage de choix au récit policier. Elle sert d'alibi pour expliquer l'absence de preuves quant à l'existence d'un soi-disant projet terroriste. Le récit policier devient alors : ces preuves existent, mais elles ne peuvent pas être déchiffrées.

Ainsi le juge d'instruction écrira que si les écoutes téléphoniques n'ont fourni que « quelques renseignements utiles », ceci s'explique par « l'usage minimaliste de ces lignes » au profit d'« applications cryptées, en particulier Signal ». Ce faisant, il ignore au passage que les analyses des lignes téléphoniques des personnes inculpées indiquent une utilisation intensive de SMS et d'appels classiques pour la quasi-totalité d'entre elles.

(...)

Il n'est pas possible de comprendre l'importance donnée à l'association de pratiques numériques à une soi-disant clandestinité sans prendre en compte le basculement de la lutte antiterroriste « d'une logique répressive à des fins préventives » dont le délit « d'association de malfaiteurs terroristes en vue de » (AMT) est emblématique. Les professeur·es Julie Alix et Oliver Cahn évoquent une « métamorphose du système répressif » d'un droit dont l'objectif

est devenu de « faire face, non plus à une criminalité, mais à une menace ».

Ce glissement vers une justice préventive « renforce l'importance des éléments recueillis par les services de renseignements » qui se retrouvent peu à peu libres de définir qui représente une menace « selon leurs propres critères de la dangerosité ».

Remplacer la preuve par le soupçon, c'est donc substituer le récit policier aux faits

(...)

Des habitudes numériques répandues et anodines sont utilisées à charge dans le seul but de créer une atmosphère complotiste supposée trahir des intentions criminelles, aussi mystérieuses soient-elles. Atmosphère dont tout laisse à penser qu'elle est, justement, d'autant plus nécessaire au récit policier que les contours des intentions sont inconnus.

À ce titre, il est particulièrement frappant de constater que, si la clandestinité est ici caractérisée par le fait que les inculpé·es feraient une utilisation « avancée » des outils technologiques, elle était, dans l'affaire Tarnac, caractérisée par le fait... de ne posséder aucun téléphone portable. Pile je gagne, face tu perds.

(...)

Face au fantasme d'un État exigeant de toute personne une transparence totale au risque de se voir désignée comme « suspecte », nous réaffirmons le droit à la vie privée, à l'intimité et à la protection de nos données personnelles. Le chiffrement est, et restera, un élément essentiel pour nos libertés publiques à l'ère numérique.

(...)

Voici comment la criminalisation des pratiques numériques s'inscrit dans la stratégie gouvernementale de répression de toute contestation sociale. Défendre le droit au chiffrement, c'est donc s'opposer aux dérives autoritaires d'un pouvoir cherchant à étendre, sans fin, les prérogatives de la lutte « antiterroriste » via la désignation d'un nombre toujours plus grand d'ennemis intérieurs.

Après la répression des personnes musulmanes, des « écoterroristes », des « terroristes intellectuels », voici venu la figure des terroristes armé·es de messageries chiffrées. Devant une telle situation, la seule question qui reste semble être : « Et toi, quel·le terroriste es-tu ? ».

L'Etat criminalise la sécurité informatique : soyons toustes Â« clandestin.es Â» ?!

Multiplier les ateliers de transmissions et de mise en pratique des divers outils de sécurité numérque

Vu que on baigne dans une société numérique, dur de se passer du monde numérique pour les activités subversives « courantes ».

Et puis, ne pas en faire partie peut aussi être une cause de suspicion...

Alors partons sur l'option 2. : qu'un maximum de monde utilise couramment des outils numériques chiffrés et sécurisés (VPN, bloqueurs de pubs et de cookies, Signal, ProtonMail, Tor, Tails, F-Droid, chiffrement de téléphone et de disque dur, etc.)

- Si un maximum de personnes plus ou moins militantes utilisent couramment des outils de sécurité numérique, ça

a deux avantages importants :

1. La sécurité de toutes ces personnes est améliorée par rapport aux intrusions de l'Etat et des boites capitalistes. Vu le durcissement et l'extension de la répression, c'est loin d'être inutile. D'autre part, ça permet d'être un peu plus autonome en informatique, de moins dépendre des multinationales et de leurs systèmes propriétaires (car souvent les outils de sécurité numérique sont des logiciels libres). (Bonus, ça limite aussi les risques de virus)
2. La sécurité des personnes les plus « engagées » qui utilisent ce type d'outils est améliorée aussi. Elles sont mieux noyées dans la masse et ne sont plus repérables dans la foule du fait de l'utilisation d'outils spécifiques.

Il faut donc multiplier les ateliers d'auto-formation, de transmissions et de mise en pratique des divers outils de sécurité numérique auprès d'un public large et diversifié. (et en même temps, de connaissances de base de l'informatique)
En fait, la plupart de ces outils ne sont pas spécialement compliqués. Il s'agit surtout d'apprendre à les connaître et de changer des habitudes.

Sans oublier que la sécurité ce n'est pas seulement les outils internet et leur utilisation, c'est un ensemble de pratiques pour l'ensemble des activités.

Projet de légalisation de la surveillance policière via tout appareil électronique

En même temps que l'Etat veut criminaliser des pratiques de sécurité numérique, il veut s'autoriser à espionner en secret via tout appareil électronique (c'est passé au Sénat et ça devrait être validé à l'Assemblée le 13 juin) :

- **Projet de légalisation de la surveillance policière via tout appareil électronique** - Big Brother n'est plus seulement dans les télécrans
Après la légalisation des drones de surveillance, voici le projet de pouvoir activer à notre insu une surveillance policière de tout appareil électronique. Téléphones mobiles bien sûr, mais aussi ordinateurs, voitures connectées, et bientôt tous les appareils électroniques connectées.

Post-scriptum :

L'Etat et les entreprises du numérique n'arrêtent pas de communiquer sur la sécurité numérique, sur les bonnes pratiques pour ne pas être piraté. Mais il ne faudrait pas que cette sécurité soit telle que l'Etat ne puisse plus Â« pirater Â» et espionner lui-même...!