Quelle est l'amplitude actuelle de la répression ?

Compilation d'exemples de répression dans les milieux militants. Analyse des moyens de surveillance à disposition des forces de l'ordre.

- Etat des lieux de la surveillance des milieux militants et des enquêtes liées
- Quels sont les moyens techniques de surveillance numérique à disposition des Forces de l'Ordre ? (Wiki en chantier □□)

Etat des lieux de la surveillance des milieux militants et des enquêtes liées

⚠ Quelques précautions avant de lire le contenu suivant:

- Les sujets suivants ne sont pas forcément comparables à répression faite sur un mouvement tel qu'Extinction Rebellion. Se reporter au chapitre Evaluer et limiter la répression pour les mettre dans le contexte.
- Toutes les méthodes d'action ne sont pas forcément en accord avec les principes d'XR dont la non-violence.
- Certaines sources sont plus fiables que d'autres.

Cependant, les sujets suivants apportant un certain éclairage sur la surveillance et les moyens d'enquête, ils semblent pertinents d'être partagés.

Enquête suite à une action contre la Fondation Louis Vuitton - 2023/2024

L'action du 1er mai 2023 consistait à recouvrir la façade de peinture de la fondation Louis Vuitton, avec quelques prises de parole. Cette enquête a été déclenchée plusieurs mois après l'action. Alors que personne n'avait été interpellée sur place, elle a conduit plus d'un an plus tard, à 4 perquisitions suivies de garde à vues, de déferrement et d'un procès.

Moyens d'enquête :

- Consultation des différents fichiers de police (TAJ, FPR, ADOC, SNPC, SIV)
- Exploitation des vidéos des médias
- Exploitation des vidéos des caméras de surveillance

- Analyses de sites web publiques (utilisation des Pages blanches pour trouver des adresses)
- Analyse du bornage sur les numéros des suspects (sans succès)
- Récupération des objets laissés sur place (sacs)
- Perquisitions avec saisies de téléphones et vêtements
- Contact d'un employeur afin d'obtenir l'adresse d'un prévenu.
- Demande d'information à des services publiques: fiches d'imposition, taxes foncières, taxes habitation
- Analyse manuelle d'un téléphone suite à un code communiqué en garde à vue.

Quelques enseignements :

- Une enquête très poussée pour une "simple action de peinture".
- Les perquistions ont été faites plus d'un an après l'action
- Il n'est pas clair de comment les prévenu.es ont été identifiées à partir des images collectées (selon les policiers "ont les connais")

Source: Analyse du dossier judidicaire.

Enquête suite à une action de Carnage Total (XR) - 2023

Cette enquête a eu lieu suite à une action coordonée de Carnage Total dans toute la France sur plusieurs dizaines d'agences bancaires BNP (groupe finançant Total) début 2023. Aucune arrestation n'a eu lieu le soir de l'action. Cependant, 6 mois après l'action, une enquête importante a été lancée qui a conduit à un procès pour 5 suspect.es.

Moyens d'enquête numériques :

- Exploitation des caméras de vidéo-surveillances des agences bancaires et des préfectures.
- Analyse poussée du bornage des téléphones et via le numéro de téléphone recoupement avec d'autres éléments pour identifier des suspect.es.
- Surveillance des réseaux sociaux (Twitter, Facebook) et des sites publiques d'Extinction Rebellion pour identifier différents auteurs potentiels.
- Analyse des réseaux sociaux de suspect.es (Facebook) pour voir les publications et comptes suivis.
- Recoupement avec les fichiers de la police/justice; par des recherches dans les procédures d'Extinction Rebellion et par recherches parmi les "complices" (pour d'autres actions) d'une personne identifiée comme suspecte sur cette action. Utilisation de la reconnaissance faciale en comparaison avec les images du fichier des Traitements des Antécédents Judiciaires (TAJ).
- Réquisitions de documents à différents organismes : CPAM, impôts, fournisseurs d'électricité, afin d'obtenir les numéros de téléphone et les adresses de suspect.es.

Moyens d'enquête physiques :

- Photos prises lors d'un évènement de soutien à un procès pour identifier de possibles auteurs.
- Perquisitions chez plusieurs suspect.es et saisies de matériels militants (téléphones, vétêments pouvant correspondre à ceux visibles sur la vidéo-surveillance, affiches, drapeaux)
- Mise en garde-à-vue, après des arrestations au domicile (vers 6h du matin) et au travail d'un suspect.

Quelques enseignements :

- Une enquête et des arrestations peuvent arriver des mois après une action.
- Selon le dossier, l'identification de certain.es suspect.es a été rendue possible grâce à des signes distinctifs (longue barbe, cheveux rasés, cheveux d'une couleur particulière). Eviter ou cacher ces signes distinctifs lors des actions peut être une bonne idée.
- Au contraire, l'identification de d'autres suspect.es a été rendu impossible du fait de masques covid portés durant l'action.
- L'analyse du bornage des téléphones a conduit à l'identification de plusieurs suspect.es. Il ne faut pas borner durant l'action mais pas non plus aux alentours de l'action (par exemple lors du trajet). Avoir un téléphone d'action avec un carte SIM non rattachée à une identité (carte SIM valable un mois) a pu permettre à certain.es suspect.es d'échapper à l'identification. Les téléphones éteints durant l'action sont présentés comme des preuves de la participation à l'action. Laissez son téléphone allumé (mais chiffré) chez soi semble plus pertinent, bien qu'un téléphone inactif ne répondant pas aux appels puisse aussi être suspect (c'est présenté comme tel dans ce dossier).
- Les photos et vidéos postées sur réseaux sociaux ont été utilisées lors de l'enquête. Nettoyer ses réseaux sociaux peut être pertinent. La communication autour de l'action doit aussi en prendre compte quand on recherche l'anonymat des militant.e.s.

Source: Analyse du dossier judidicaire.

Enquête suivant le désarmement de l'usine Lafarge de Bouc-Bel-Air - 2022

Se reporter à l'analyse partagée par Les Soulèvements De La Terre .

Enquête policière pour retrouver les activistes des Soulèvements de la Terre

ayant désarmé.es une méga-bassine - 2022

L'enquête préliminaire sur des personnes soupçonnées d'avoir désarmées une mégabassine semble avoir été très poussée avec entre autre:

- les données administratives des suspects épluchées: leurs relevés d'imposition, de CAF ou d'assurance maladie disséqués
- L'analyse de leurs données téléphoniques: leurs factures téléphoniques, les fadettes (bornages des téléphones)
- Enquête sur l'entourage des suspects

Sources: Libération: Mégabassines, comment la justice traque les militants écolos

Enquête policière contre "Youth for Climate" - 2020

En 2020, un collectif baptisé L'Arche, au sein duquel on retrouve des membres de Youth for Climate, proteste contre la gentrification du quartier Sainte-Marthe et organisent plusieurs actions dont l'occupation un local d'un restaurant vide depuis des années.

Pour les poursuivre en justice, la police a alors créé un dossier de plus de 1000 pages contenant entre autre:

- l'analyse du contenu posté sur les réseaux sociaux dont Instagram. Les visages étaient floutés mais l'identification de personnes a tout de même été possible grâce à l'observation des vêtements.
- l'analyse du bornage des téléphones à proximité de la zone afin d'identifier les personnes présentes lors de l'action.
- l'identification du créateur (par son IP) d'une adresse e-mail Protonmail suite à la saisie de la justice Suisse.

Sources: paris-luttes.info: Récit policier de Saint Marthe, paris-luttes.info : Communiqué sur l'affaire de la place Saint Marthe, secours-rouge.org, francetvinfo.fr

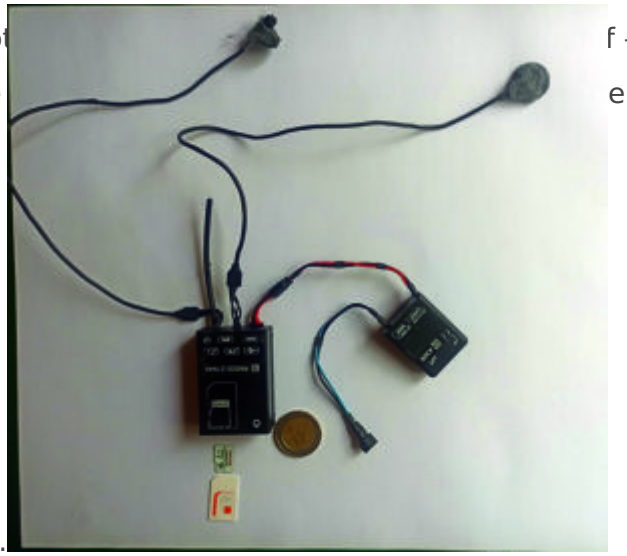
Surveillance massive des militant.e.s antinucléaire à Bure - 2017/20

L'article de Reporterre, Reporterre: La justice a massivement surveillé les militants antinucléaires de Bure, démontre une surveillance massive des militant.es antinucléaire à Bure.

Quelques éléments pour se rendre compte de l'ampleur de la surveillance:

- Des dizaines de personnes placées sur écoute
- un millier de discussions retranscrites
- plus de 85.000 conversations et messages interceptés
- plus de 16 ans de temps cumulé de surveillance téléphonique
- 118 personnes fichées dans l'organigramme versé dans le dossier d'instruction

Mise sur écoute d'une bibliothèque Anarchiste à Paris - 2022

La mise sur écoute de la bibliot  f – 75019 Paris) a été documenté dans cet article de e a été découvert dans une imprimante en Mars 2022.

D'autres exemples de ce genre peuvent être trouvés sur : https://www.notrace.how/earsandeyes

Surveillance sur les réseaux sociaux des critiques de LVMH - 2021

Selon une enquête de Politico, les réseaux sociaux des personnes critiquant le PDG du groupe LVMH, Bernard Arnault, dont l'organisation Altermondialiste Attac et des militant.e.s ont été surveillés par une entreprise privée.

Enquête sur des actions anarchistes - 2008

Six personnes ont été mises en examen pour divers motifs allant de la détention de fumigènes et de clous crève-pneus en manifestation en passant par la détention de produits pouvant rentrer dans la confection d'explosifs.

Le dossier d'instruction de 2008 (à garder en tête les techniques d'enquête ont évoluées) de plus de 6000 pages révèle que la police a:

- fait des enquêtes sur les profils des accusés grâce à: des enquêtes de personnalité, des expertises psychologiques et psychiatriques, des interrogatoires des parents
- fait des prélèvement d'ADN dans une maison utilisée comme lieu de rassemblement par des militant.e.s anarchistes.
- analysé les ordinateurs, disques durs, clés USB et téléphones saisis.
- prélevé l'ADN en garde à vue sur les vêtements et gobelets des suspects
- rédigé des procès verbaux sur les discours tenus entre les suspects dans leurs cellules durant la garde à vue.
- mise sur écoutes plusieurs lignes téléphoniques.
- analysé une carte SIM saisie permettant d'obtenir les informations suivantes:
  - le nom et le pays de l'opérateur ayant délivré la carte
  - le numéro identifiant de l'abonnement du mobile (IMSI)
  - le répertoire téléphonique
  - les messages SMS, effacés ou non, avec leur statut : « reçu et lu », « reçu et à lire », « à envoyer », « envoyé » et les « accusés réceptions »
- analysé la messagerie vocal d'un numéro de téléphone et ce même si le message a été supprimé.
- analysé les composants chimiques du fumigène
- pris de très nombreuses photos lors de rassemblement anarchistes

Source: Infokiosques: Analyse d'un dossier d'instruction contre des anarchistes

Traçage GPS du véhicule du porte parole de "Bassines - Non Merci" - 2023

- traçage GPS en temps réel par un petit boîtier noir dissimulé sous l'essieu de son véhicule
- surveillance assumée à regret par la préfecture

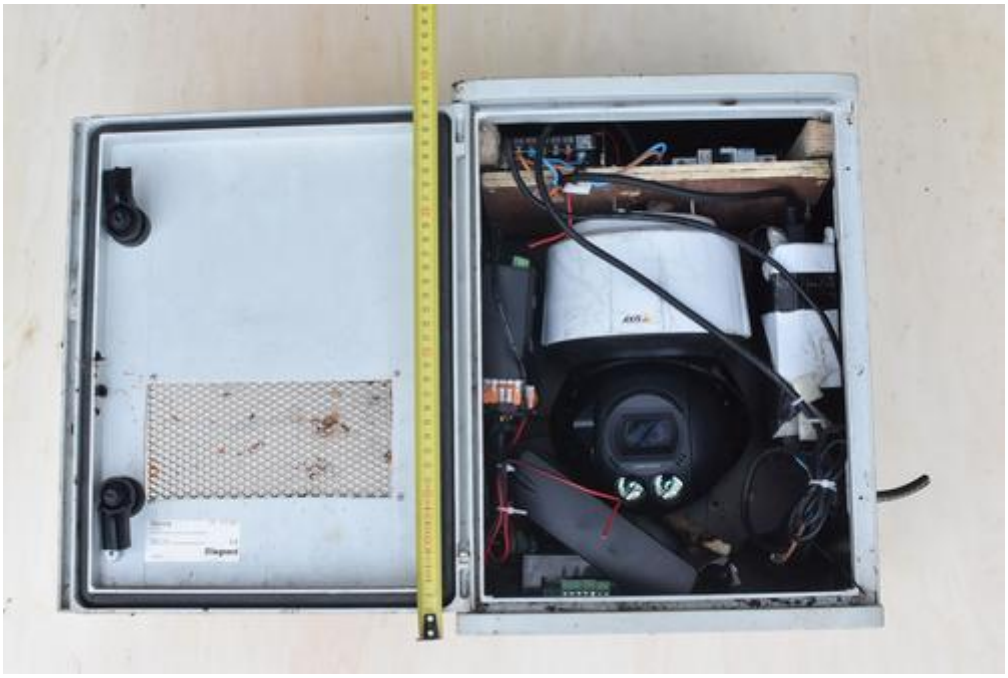
Source: Article Dijoncter.info par Les Soulèvements de la Terre

D'autres exemples de ce genre peuvent être trouvés sur : https://www.notrace.how/earsandeyes

Vidéosurveillance de lieux autogérés - 2022

Vidéo surveillance sur plusieurs mois des accès véhicule et piéton et parking de 2 lieux autogérés à Dijon.

- boîtiers (voir ci-dessous) attachés au sommet de poteaux électriques
  - caméra à globe orientable
  - alimentation raccordée au poteau électrique => autonomie illimitée



Source: Article Dijoncter.info + photos des champs des caméras

D'autres exemples de ce genre peuvent être trouvés sur : https://www.notrace.how/earsandeyes

Quels sont les moyens techniques de surveillance numérique à disposition des Forces de l'Ordre ? (Wiki en chantier □□)

Vers où tendent les moyens techniques ?

Les autorités françaises étaient en 2020 dans les dernières étapes de négociations pour l'achat du système de surveillance Pegasus avant d'y renoncer. Bien que l'achat ne se soit pas fait, cela montre la volonté des autorités françaises d'obtenir les moyens techniques de surveillance les plus poussés.

Qu'est-ce que le logiciel espion Pegasus ?

Le superviseur européen de la protection des données a publié un rapport très complet sur Pegasus.

Pour résumer, Pegasus est* le logiciel espion connu le plus performant et cela pour les raisons suivantes:

- il donne un accès total au téléphone espionné. Il a accès à aux caméras, aux micros, aux fichiers, aux applications, etc.
- il peut infecter un appareil avec une attaque "Zéro Click" c'est-à-dire sans aucune action de la victime. Donc quelque soit votre vigilance, si vous êtes visé.es vous ne pouvez pas empêcher l'infection de votre téléphone.
- il est indétectable par l'utilisateur et seule une analyse technique très poussée a permit d'identifier les téléphones infectés.

Ce logiciel espion a notamment été utilisé en Europe contre des citoyen.ne.s européen.nes incluant des journalistes, des politiques, des avocat.es.

*: Suite aux enquêtes, les failles de sécurités utilisés par Pegasus ont été réparées par les entreprises logiciels (Google et Apple). Si vous avez sur votre smartphone la dernière version du système d'exploitation, il est possible que vous soyez protégé.e. Cependant, les fabricants de téléphone (autres que Apple et Google) proposent rarement la dernière version du système d'exploitation. Votre téléphone est donc probablement toujours vulnérable. De plus, d'autres failles non détectées pourraient être utilisées. Il semble donc pertinent de considérer que le logiciel espion Pegasus est encore efficace et utilisé.

Quelles sont les pratiques et outils de hacking des FDO ?

Selon un rapport de 2017 demandé par le parlement européen, les enregisteurs de frappe ou Key Logger, c'est-à-dire un système qui enregistre l'utilisation d'un ordinateur ou téléphone cf: wikipedia, sont les outils les plus utilisés par les Forces De l'Ordre. En 2017, ce rapport concluant que les outils de "hacking" n'étaient pas énormément utilisés.

Selon un autre rapport du Superviseur européen de la protection des données de 2013, la France a un système de surveillance de masse en collectant directement les données sur les infrastructures. Cependant en 2013, les moyens étaient bien plus faibles que les agences de surveillance américaines et Britanniques. La France était alors considéré comme le 5ième pays collectant le plus de metadonnées.

Cadre légal du hacking en France

En France, les techniques de piratage informatique sont autorisées par les articles 706-102-1 et 706-102-2 du Code de procédure pénale. Elles permettent entre autre aux forces de l'ordre d'accéder à distance aux ordinateurs et autres appareils.

En vertu de l'article 706-102-1, les opérations ne peuvent être autorisées que pour une période maximale d'un mois. Le renouvellement est possible une fois dans les mêmes conditions.

En vertu de l'article 706-102-2, les opérations sont autorisées pour une durée plus longue, dans la limite d'une période initiale maximale de quatre mois, renouvelable dans les mêmes conditions dans la limite d'une période totale de quatre mois.

La gouvernance diffère selon ces dispositions puisque l'article 706-102-1 concerne les enquêtes menées par le procureur de la République, alors que l'article 706-102-2 concerne les enquêtes menées par le juge d'instruction.

Le hacking peut être utilisé par les fdo pour les crimes avec des peines d'au moins 2 ans de prison.

Pour rappel, de nombreuses méthodes d'action de DCNV (par exemple l'entrave à la circulation) peuvent théoriquement conduire à des peines de prison de 2 ans ou plus. **Le "hacking" est donc légal pour prévenir des actions de DCNV**.

A noter, l'article 163 garantit un inventaire judiciaire des preuves électroniques pouvant être exploitées par des experts techniques. Il précise que les experts qui effectuent des opérations d'exploitation doivent rédiger un rapport qui contient une description des opérations et leurs conclusions. L'inventaire et les rapports sont fournis à la juridiction et enregistrés dans le procès-verbal. Si procès, il peut donc être intéressant de vérifier la présence d'un tel procès-verbal.