Que peut faire la police avant l'action ?

> Sur la surveillance et **ce que peut faire la police en matière d'investigations numériques**, on peut surtout noter cet article très complet disponible sur paris luttes info (notamment) : https://paris-luttes.info/fadettes-ufed-et-donnees-de-16236

S'il y a de la surveillance en amont d'une action, cette surveillance n'est pas réalisé par la police judiciaire mais **par les services de renseignement**. En effet, la police judiciaire n'intervient qu'après, par rapport à des infractions déterminées (cf la partie sur l'enquête et l'exception de l'association de malfaiteurs). Les services de renseignement ont uniquement vocation à prévenir les atteintes, pas à les sanctionner. Pour répondre à la question des moyens que peut mettre en place la police en amont d'une action, il faut donc s'intéresser aux services de renseignement et à leur cadre légal.

Les services de renseignement : de quoi parle-t-on ?

On parle régulièrement de "RT" (ou "RG") pour **"renseignements territoriaux"**. Il s'agit de policiers du service central du renseignement territorial, qui sont rattachés à la direction générale de la police nationale. Ils sont chargés "d'exploiter les renseignements concernant tous les domaines de la vie institutionnelle, économique et sociale afin d'apporter un éclairage aux autorités et pouvoirs publics sur ces sujets, en particulier ceux susceptibles d'entraîner des mouvements revendicatifs ou protestataires [...] ainsi que la contestation politique violente."

En plus de ce maillage territorial, le service national de renseignement est la **direction générale de la sécurité intérieure** qui, lui, est rattaché directement au ministère de l'intérieur est constitue à proprement un service de renseignement "du premier cercle". Il est chargé "de rechercher, centraliser et exploiter le renseignement intéressant la sécurité nationale ou les intérêts fondamentaux de la nation".

On peut aussi noter d'autres services de renseignement, comme la **direction du renseignement de la préfecture de paris**, ou encore la sous-direction de l'anticipation opérationnelle de la gendarmerie nationale. Bref, il y en a tout plein.

Ces services ont pour objet la "collecte, le traitement et l'exploitation d'informations stratégiques, afin d'assurer la défense des intérêts de la Nation, relèvent des prérogatives des

services de renseignement français". Concrètement, ces informations peuvent servir à **empêcher des actions**, à **mettre sous surveillance** renforcée (voire à assigner à résidence) des personnes leur apparaissant comme particulièrement impliquées, ou **être utilisées a posteriori dans une procédure judiciaire**.

Les moyens que peuvent théoriquement utiliser les services de renseignement sont très vastes : **balisage de véhicule**, sonorisation de lieux privés (**micros**), captation d'images dans des lieux privés (**caméras**), captation de **données informatiques**, **géolocalisation**, accès aux réseaux des opérateurs de télécommunications (**SMS, appels téléphoniques, sites consultés via données mobiles**) et à toutes les correspondances téléphoniques (ce qui rend signal safe est donc uniquement l'impossibilité technique à en déchiffrer les messages), brouillage de drones, utilisation des imitateurs d'antennes relais ("IMSI catcher") qui permettent d'aspirer les conversations téléphoniques dans un périmètre donné, **logiciels espions** sur les téléphones et ordis (accès à toutes les frappes clavier de l'ordinateur - dont les mots de passe -, captures d'écrans en temps réel, accès à la webcam et au micro de l'ordinateur...) mais aussi **algorithmes** permettant de repérer via les données de connexion et de navigation des opérations suspectes.

En plus de ces moyens "extraordinaires" en ce qu'ils portent atteinte à notre vie privée, iels peuvent aussi évidemment utiliser des **moyens plus classiques** pour récupérer des infos : **recherches sur internet, rejoindre des groupes, venir à des briefs, s'inscrire sur nos outils, venir à des moments informels...**

Cadre légal et limites

Les services de renseignement sont encadrés par un cadre légal.

Globalement, ces services sont censés respecter le **droit au respect de la vie privée**, qu'iels peuvent cependant outrepasser pour "la défense et la promotion d'intérêts fondamentaux de la Nation".

Ce qu'iels ont le droit de faire (le cadre légal)

- Les accès administratifs aux données de connexion, qui comprennent :

  - les accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure),
  - les accès aux données de connexion en temps réel (article L. 851-2 du code de la sécurité intérieure),
  - la mise en œuvre de traitements automatisés sur les seules données de connexion acheminées par les réseaux des opérateurs de communications électroniques ou des fournisseurs de services en ligne (article L. 851-3 du code de la sécurité intérieure),

- la géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure),
- le balisage (article L. 851-5 du code de la sécurité intérieure),
- le recueil de données de connexion par *IMSI catcher* (article L. 851-6 du code de la sécurité intérieure) ;

- Les interceptions de sécurité :

- l'interception des communications acheminées par les réseaux des opérateurs de communications électroniques ou des fournisseurs de service en ligne (article L. 852-1 du code de la sécurité intérieure),
- l'interception des communications échangées au sein d'un réseau privatif empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques (article L. 852-2 du code de la sécurité intérieure ;
- la captation de paroles prononcées à titre privé (article L. 853-1 du code de la sécurité intérieure) ;
- la captation d'images dans un lieu privé (article L. 853-1 <du code de la sécurité intérieure) ;
- le recueil ou la captation de données informatiques (article L. 853-2 du code de la sécurité intérieure.

L'introduction dans un lieu privé, ce qui inclut les lieux à usage d'habitation, peut être autorisée, par décision spécifique, à la seule fin de mettre en place, utiliser ou retirer un dispositif de balisage, de captation de paroles, de captation d'images, de recueil ou de captation de données informatiques (article L. 853-3 du code de la sécurité intérieure).

La surveillance des communications émises ou reçues à l'étranger fait l'objet de dispositions particulières (articles L. 854-1 à L. 854-9 du code de la sécurité intérieure).

Enfin l'interception des communications échangées au sein d'un réseau ouvert empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques est autorisée et limitée à un champ d'application résiduel (articles L. 855-1 A à L. 855-1 C du code de la sécurité intérieure).

Source : https://www.cnctr.fr/3_cadre_legal.html

La légalité des moyens de renseignement est censée être **contrôlée par une autorité indépendante**, la Commission nationale de contrôle des techniques de renseignement (CNCTR). **Certains actes** (accès aux données de connexion, interceptions de sécurité, sonorisation de certains lieux et véhicules, captation d'images et de données informatiques et des mesures de surveillance des communications électroniques internationales) **sont soumis à l'avis de cette commission avant d'être autorisés par le premier ministre, à titre exceptionnel.**

Et concrètement ?

Dans les faits, pour citer l'article de paris luttes info :

"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, 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."

En France en 2018, l'année des gilets jaunes, 22 000 personnes ont été placées sur écoutes (appels téléphoniques mais pas uniquement, aussi pages webs consultés avec données mobiles, sms...) 9 % de ces écoutes concernaient des faits de « violences collectives », donc, en gros, « d'émeute ».

On peut aussi penser, plus récemment, aux moyens de surveillance massifs mis en place pour l'action concernant les méga-bassines à Ste Soline fin octobre 2022 : drones, hélicoptères..., ou à l'annonce de Darmanin selon lequel il y aurait eu une quarantaine de fichés S à Ste Soline.

> Comment savoir si je suis surveillé.e par les services de renseignement ? C'est a priori impossible ; la seule chose que vous avez la possibilité de faire est de demander à ce que la CNCTR vérifie la légalité des méthodes de renseignement qui sont mises en place à votre encontre, sans que vous ne sachiez si de telles méthodes sont effectivement mises en place.
>
> Plus d'infos par ici.

Révision #5
Créé 6 mai 2023 00:41:40 par alice
Mis à jour 21 mars 2024 23:24:52 par alice