... transmettre quelques infos sur les tactiques des flics et sur leurs possibilités techniques. L'objectif étant bien sûr d'inciter d'autres à en faire de même car collectiviser ces infos ne peut que nous renforcer afin d'être prudents dans nos actes politiques sans tomber dans la paranoïa.

BEAUCOUP D'INFOS SUR
HTTP://INFOKIOSQUES.NET/MAUVAISES_INTENTIONS

— mai 2010 —

Analyse d'un dossier d'instruction antiterroriste

CES QUELQUES PAGES TRAITENT du dossier d'instruction judiciaire sur ce qui fut, en janvier 2008, la première affaire traitée par une juridiction antiterroriste concernant ce que policiers, juges et médias nomment « la mouvance anarcho-autonome », plus spécifiquement dans cette histoire « la mouvance anarcho-autonome francilienne ». Dans cette affaire, six personnes ont été mises en examen et ont fait de 4 à 13 mois de prison. Les faits reprochés sont divers : détention de fumigènes et de clous crève-pneus en manifestation, tentative d'incendie d'une dépanneuse de police, détention de produits pouvant rentrer dans la confection d'explosifs (chlorate de soude), détention de manuels de sabotages et de plans d'une prison pour mineurs (l'EPM de Porcheville). Ces six personnes sont maintenant soit sous contrôle judiciaire, soit en fuite ; aucune date de procès n'a été fixée. Pour rappel sur ces histoires : **HTTP://INFOKIOSQUES.NET/MAUVAISES_INTENTIONS**

Il semblerait même que la justice n'ait pas du tout envie d'accélérer la procédure, le parquet a récemment prétendu avoir retrouvé une trace ADN de l'un des mis en examen sur un sabotage datant du mouvement anti-CPE de 2006, soit 4 ans après les faits et 18 mois après avoir prélevé son ADN. L'instruction a donc été rouverte. Pour rappel : HTTP://NANTES.INDYMEDIA.ORG/ARTICLE/19423

Nous essayons donc dans cet article de reprendre et de résumer quelques éléments intéressants de cette instruction, tant d'un

point de vue technique que d'un point de vue théorique. Il va sans dire que de nombreuses réserves doivent être soulignées dans ce type de démarches. D'un point de vue technique nous recopions des passages figurant dans l'instruction, écrits par des flics, des experts ou des juges (indiqués dans l'article entre « » et en italique). Nous ajoutons aussi des résumés ou des explications et interprétations écrits par nous-mêmes. Cela ne signifie évidemment pas que tous les dossiers sont similaires de ce point de vue. Surtout cela ne signifie pas que les flics ne soient pas capables de bien d'autres choses que ce qui est écrit. Par exemple dans notre dossier, il n'est jamais question de balises sur des voitures ou de micros dissimulés dans des appartements ; des techniques qui ont été utilisées dans d'autres affaires. Cela ne signifie pas non plus qu'ils ne l'aient pas fait dans notre affaire et que cela ne figure pas dans le dossier judiciaire. Bref, d'une manière générale les quelques exemples figurant dans ce dossier ne doivent pas être pris comme des généralités. Cet article présente quelques exemples figurant dans un dossier spécifique et rien de plus. Il nous a semblé néanmoins intéressant de publier et de partager ces quelques éléments, qui n'ont rien de bien neufs en soi, avec tous ceux qui un jour ou l'autre peuvent se retrouver dans des situations similaires.

Nous pensons d'ailleurs qu'il serait intéressant que ceux qui ont accès à des dossiers dans d'autres affaires en fassent de même, surtout quand ces dossiers concernent directement ou indirectement bien plus de monde que les seuls mis en examen. Nous pensons évidemment en premier lieu aux inculpés de l'affaire dite de « Tarnac » qui n'ont jamais fait clairement cette démarche envers tous ceux qui pourraient être concernés tout en laissant le dossier entièrement ouvert à pleins de crapules journalistiques de passage (*Le Monde* dès mars 2009, *L'Express, Libération*…). Cette distorsion en dit long sur l'état d'esprit des mis en examen de cette affaire face à la justice, mais il est certain que les médias que nous avons cités sont les mieux placés pour faire passer leur discours démocrate policé sur les gentils petits étudiants que le méchant juge Fragnoli empêche de planter tranquillement des carottes. Et qu'on ne s'y méprenne pas, il n'est nullement ici question de régler des comptes mais de souligner l'inconséquence politique très grave de laisser des

Concernant des actes commis, ils font des localisations ciblées de téléphones a posteriori appartenant à des gens soupçonnés, qui leur donnent l'endroit où le téléphone a borné à telle heure de tel jour. Ils visionnent quelques caméras aux alentours de la découverte d'un engin incendiaire (en l'occurrence, des caméras d'un distributeur de La Poste). Ils analysent s'il reste des traces d'empreintes digitales (qu'ils appellent empreintes papillaires) sur la dépanneuse en question. Ils font une enquête de voisinage assez poussée dans les immeubles alentours. Ils referont également une enquête de voisinage conséquente autour d'une maison secondaire, cette fois là davantage dans un objectif de renseignements qu'en lien avec un acte précis. Ils saisissent et reproduisent avant de les transmettre au destinataire plusieurs courriers envoyés de détention ou reçus en détention, en ajoutant des traductions si les courriers ne sont pas en français. En détention et pendant une instruction, tout le courrier envoyé de et en détention est lu à la fois par l'Administration pénitentiaire et par le juge d'instruction, et certains courriers sont reproduits dans le dossier.

Des appareils photos saisis en perquisition sont exploités ainsi que des clés USB et des disques durs d'ordinateur. Concernant ces derniers, leur processus d'expertise est un peu moins clair. Il est évident qu'ils retrouvent tout ce qui n'est pas crypté, même ce qui a été effacé. On remarque que si au milieu d'un ordinateur, ils notent des fichiers cryptés, leur attention va en priorité vers ces dossiers qu'ils transmettent en vue d'être décryptés. Sur ce point on ne parvient pas à tirer de conclusions très claires de ce qu'ils parviennent ou non à décrypter et nous préférons donc ne pas en tirer de conclusions.

Voilà quelques éléments de ce dossier, cet article est loin d'être exhaustif mais vise comme nous l'avons dit en introduction à transmettre quelques infos sur leurs tactiques et sur leurs possibilités techniques. L'objectif étant bien sûr d'inciter d'autres à en faire de même car collectiviser ces infos ne peut que nous renforcer afin d'être prudents dans nos actes politiques sans tomber dans la paranoïa.

A bon entendeur…

de référence ne proviennent pas de la même personne et que, par le fait du hasard, un autre individu possède la même empreinte génétique que la personne dont provient l'ADN de question. ***Pour chaque locus étudié, on calcule donc la probabilité de trouver, dans la population générale, un individu possédant ces deux allèles.***

On associera à l'affirmation d'identité la probabilité de trouver, dans une population prise au hasard, un individu possédant le même profil génétique que la personne dont provient l'ADN en question pour tous les locus testés.

Les fréquences sont extraites d'études de populations publiées dans des revues internationales et d'une étude de la population française effectuée en laboratoire.

Quelques extraits de conclusions :

(Suite à un prélèvement de l'ADN de X), L'empreinte génétique de X à été caractérisée sur ***une taie d'oreiller, une brosse à dent, un drap****. La fréquence de cette empreinte génétique dans la population générale est de un sur 96 millions de milliards. Donc la justice en conclut que les traces ADN retrouvées sur la taie d'oreiller, la brosse à dent et le drap appartiennent à l'individu X en question.*

Nantes, juin 2008

Rapport d'expertise à destination du Tribunal de Grande Instance de Paris – Section antiterroriste

Docteur Olivier Pascal et Alexandra Schlenck- Institut Français des Empreintes Génétiques – Site de la Géraudière – Rue Pierre Adolphe Bobierre – BP 42301 – 44323 Nantes Cedex 3 Tél : 02.72.64.21.95 / Fax : 02.72.64.71.70 »

Voici enfin un certain nombre d'autres actes de procédure qui donnent une idée de l'étendue de leurs possibilités sur lesquelles on ne s'attarde pas plus, soit parce qu'il n'y a pas grand-chose à en dire, soit parce qu'on n'a pas pris plus de temps pour le faire.

Par exemple, il y a plusieurs PV concernant des dialogues tenus en garde à vue, qui disent que les gens se mettent d'accord sur une version en se parlant d'une cellule à l'autre. Lors de plusieurs gardes à vue de personnes soupçonnées, ils prennent l'ADN sur des habits (pulls, caleçons) ou sur un gobelet par exemple. On note que lors d'une procédure d'urgence dans une garde à vue, ils mettent 9 heures pour comparer un ADN prélevé sur le gardé à vue avec un ADN retrouvé sur un engin incendiaire un an plus tôt.

médias avoir accès à des données parfois sensibles ou intimes d'une instruction tout en refusant de le faire pour les proches qui peuvent être directement concernés.

Cet article ne prend pas en compte le récent ajout au dossier de la procédure concernant les sabotages SNCF durant le mouvement anti-CPE, nous nous limitons à la tentative d'incendie d'une dépanneuse de la police en mai 2007 et aux arrestations de janvier 2008. Ce qui signifie qu'il y a peu d'éléments de ce qu'on appelle une « enquête préliminaire », ou du moins d'une enquête avant les arrestations, et qui sont souvent les éléments les plus intéressants.

D'une manière générale dans un dossier, les pièces arrivent au fur et à mesure au greffe du tribunal selon le bon vouloir du juge d'instruction et du parquet, c'est d'ailleurs une de leurs techniques de tarder à transmettre des pièces qui ne vont pas dans leur sens. Par exemple dans notre histoire, deux personnes ont été arrêtées en janvier 2008 avec un fumigène en allant à une manifestation. Au bout de 24 heures de garde à vue une sorte de pré-expert avait déjà expliqué qu'il s'agissait d'un produit explosif, ce qui les arrangeait bien sur le moment pour gonfler l'histoire. Ensuite, la véritable expertise, admettant à demi-mot que ce mélange n'était pas explosif et était sans doute destiné à être consumé pour produire de la fumée, a été transmise à la défense au bout de sept mois. Entre-temps, l'affaire était passée à la juridiction anti-terroriste et deux copains avaient fait plus de quatre mois de prison chacun.

Les pièces arrivant sous forme papier ou informatique sont classées en cotes. Une cote peut comporter de une à cent pages, cela dépend. Notre dossier comprend 840 cotes, soit environ plus de 5000 pages. C'est un aspect important, les dossiers sont longs, très chiants à lire, remplis d'inepties procédurières, genre des pages entières qui pourraient se résumer par : « *Le mardi 7 avril, Julien Mabrut, troufion policier, a tenté de prendre contact avec Sandrine Valade, troufion expert, mais ça répond pas. Dont acte.* ». Il faut donc une certaine habitude pour distinguer ce qui est intéressant et ce qui est purement procédurier. On se décourage rapidement devant des milliers de pages, c'est sans doute

l'un des objectifs, et pourtant il est évidemment très important qu'un mis en examen connaisse parfaitement son dossier et ne s'en remette pas à son avocat, qui d'ailleurs ne lit pas très souvent les dossiers.

De plus, au-delà de tout cet aspect procédurier, le dossier est parsemé d'incohérences plus ou moins voulues, et de directions d'enquêtes qui peuvent sembler absurdes au premier regard. Par exemple la présence d'un autocollant de Georges Ibrahim Abdallah sur le frigo d'un lieu perquisitionné va justifier des pages entières de renseignements sur lui et sur tous ses potes. Ou la découverte d'un article concernant l'EZLN (armée zapatiste au Chiapas) sur un ordinateur qui entraîne une dizaine de pages copiées-collées de wikipedia sur Zapata qui aura sans doute valu une très bonne note au flic en charge de cet exposé. Alors bien sûr il faut être prudent et la justice peut se servir de ces prétextes (autocollant, article sur un ordinateur…) pour donner une connotation au dossier dans le sens désiré, mais clairement les directions d'enquêtes semblent aussi être laissées à l'intuition du juge d'instruction qui ne sort jamais de son bureau. Dans d'autres exemples, on se rend compte que parfois les flics s'intéressent à quelqu'un en particulier et que pour des raisons pas très claires ils vont mettre les moyens pour le retrouver et l'interroger et que dans d'autres cas, ils laissent tomber après avoir passé quelques coups de téléphone infructueux. Il nous semble qu'il n'y a vraiment pas de généralités ni de cohérence très claire d'ensemble. D'une manière générale, l'aspect procédurier et intuitif des directions d'enquêtes nous semble très présent dans ce dossier. Ce dossier vient renforcer également une évidence, il faut se garder de ne pas tomber dans des logiques extrêmes qui voudraient soit que les flics sont complètement à la masse et ne comprennent rien à rien, soit qu'ils sont omniscients et qu'avant même le début de l'enquête ils savent déjà tout.

Il est aussi important de souligner que les enquêtes visent bien plus que des faits spécifiques reprochés, ils enquêtent au moins autant sur des profils à travers des enquêtes de personnalité, des expertises psychologiques et psychiatriques, des interrogatoires des parents… Cette démarche existe dans toute procédure criminelle. De plus dans notre affaire ils passent aussi du temps à tenter d'établir des liens entre des personnes, des groupes. Par

*Annexe : typage **ADN nucléaire***

L'ADN composant les chromosomes qui se trouvent dans le noyau des cellules (l'ADN nucléaire) comporte des régions variables d'individu à individu. Ces régions sont composées d'unités de base constituées de deux à plusieurs centaines de nucléotides. Les techniques de biologie moléculaire permettent d'extraire l'ADN et de visualiser ces régions particulières (les locus). Nous utilisons la technique d'amplification (ou PCR : Polymerase Chain Reaction) pour étudier des courtes régions variables de l'ADN appelées STR (Short Tandem Repeat). Les unités de base des STR sont constituées de 2 à 7 nucléotides. Le nombre de nucléotides par répétition est stable pour un même locus, mais le nombre de répétitions varie, entraînant l'existence pour un même locus de nombreux fragments d'ADN (allèles) se différenciant par leur taille. La majorité des locus retenus par la communauté scientifique pour l'établissement d'empreintes génétiques est composée d'unités de base de 4 nucleotides. Après une extraction d'ADN spécifique au matériel de départ (sang, salive, mégots de cigarettes, tâches biologiques…), la région d'intérêt est encadrée par des bornes, des amorces puis copiée, amplifiée par une enzyme particulière.

La technique d'amplification (PCR) est une technique particulièrement sensible. De ce fait, des analyses peuvent être effectuées sur des quantités très faibles de matériel biologique (petite tâche de sang ou de sperme, mégot de cigarette, bulbe de cheveux…). Cependant, une quantité minimale de 50 à 100 cellules (0,5 ng d'ADN) est nécessaire pour obtenir un résultat interprétable.

Ces analyses permettent également de mettre en évidence des mélanges d'ADN (en cas de viol par exemple). Toutefois les proportions trop faibles d'un ADN par rapport à l'autre ou l'existence de mélanges complexes de plusieurs ADN (viols multiples par exemple) peuvent entraîner des difficultés d'interprétation.

Interprétation des résultats – identification des individus

Nous avons à notre disposition deux types de prélèvements : les prélèvements de question (ADN inconnus) et les prélèvements de référence (ADN dont l'origine est identifiée). Pour chaque région de l'ADN, le même raisonnement est suivi. Si les allèles cara-ctérisant l'ADN de question sont différents des allèles caractérisant l'ADN de référence, les deux ADN proviennent, de façon certaine, de deux individus distincts. ***Si les deux allèles sont identiques pour les deux ADN, il est probable qu'ils proviennent du même individu.***

Néanmoins, la totalité de l'ADN n'étant pas analysée, on peut imaginer que plusieurs personnes puissent posséder le même profil génétique pour les régions analysées. Dans ce cas, l'hypothèse est que l'ADN de question et l'ADN

chondrial sera préconisée dans les cas d'échantillons biologiques en quantité très limitée ou fortement dégradés. L'ADN est aussi présent dans les cheveux ou autres éléments pileux sans bulbe (où l'ADN nucléaire n'est pas détectable). Cet ADN présente des variations entre individus, mais à un degré moindre comparé à l'ADN nucléaire. De plus, les mitochondries étant héritées uniquement de la mère, ***les individus d'une même lignée maternelle posséderont le même ADN mitochondrial et ne pourront pas être distingués.***

Deux régions variables de l'ADN mitochondrial sont copiées par la technique d'amplification d'ADN puis sont séquencées, c'est-à-dire que le code génétique est décrypté nucléotide par nucléotide sur environ 600 nucléotides. Les points de variations (mutations) observés dans cette séquence par rapport à une séquence de référence permettent de caractériser l'ADN.

La comparaison s'effectue, soit avec un ADN mitochondrial d'une autre source biologique du même individu, ***soit avec un ADN mitochondrial provenant d'un individu de la même lignée maternelle.*** *L'identité est établie si les deux ADN présentent les mêmes variations de séquence nucléotidique.*

En cas d'identité de deux séquences d'ADN mitochondrial, il est indiqué que ces deux ADN proviennent de la même personne ou de deux personnes apparentées par la ligne maternelle. Le résultat est accompagné d'une indication de la fréquence de cet ADN dans une banque de données internationale comprenant les séquences de 4360 individus non apparentés. Certaines séquences d'ADN mitochondrial sont fréquentes et constituent 2,6% des séquences de la banque de données.

Dans ce cas, nous considérons que cette forte représentation ne permet pas une inclusion fiable et que seule une exclusion sera possible. *L'ADN mitochondrial est plus sensible que l'ADN nucléaire aux erreurs de réplication. De ce fait, il peut exister chez un même individu un mélange de deux populations d'ADN mitochondriaux présentant une différence de séquence pour un nucléotide précis. La proportion de ces populations peut varier entre différents types de prélèvements (éléments pileux, sang…) chez un même individu. Ce phénomène est connu sous le nom d'hétéroplasmie. Du fait du phénomène d'hétéroplasmie, une exclusion ne sera affirmée que lorsque les échantillons comparés présentent des ADN mitochondriaux avec au moins deux différences de séquence.*

Deux remarques importantes : l'analyse de l'ADN mitochondrial ne permet pas de déterminer le sexe de la personne dont provient l'ADN. Le séquençage de l'ADN mitochondrial est la seule technique de biologie moléculaire utilisable pour les éléments pileux sans bulbe et pour les échantillons biologiques fortement dégradés ou en quantité très faible.

exemple, dans une maison de campagne qu'ils ont liée à notre affaire, plus d'une dizaine d'ADN nucléaires inconnus ont été relevés et placés au fichier des empreintes génétiques (FNAEG) en attente d'être recoupés.

Nous l'écrivons avec les précautions habituelles mais nous avons noté dans notre dossier que les informations dites « de première main » (sous-entendu les infos directement récoltées par les flics sur le terrain, par d'éventuels indics, par les RG…) sont très peu nombreuses. L'essentiel de leurs infos et du contenu de leurs fiches de renseignements transmises concernent le recoupement d'informations policières et administratives : contrôles d'identité, gardes à vue… Toutefois cette histoire date maintenant d'il y a deux ans et on peut s'imaginer que leurs connaissance de terrain se soient améliorées depuis.

Il est difficile de distinguer avec précision ce qu'implique concrètement une instruction antiterroriste par rapport à une autre instruction. Il est évident que c'est en grande partie un effet d'annonce politique qui a été déjà analysé (cf HTTP://INFOKIOSQUES.NET/MAUVAISES_INTENTIONS). Sans doute l'instruction est elle rallongée, sans doute les logiques soulignant l'existence d'une organisation avec ses chefs, ses mots d'ordre, ses consignes est-elle accentuée ; sans doute une attention spécifique est dédiée aux mis en examen en détention et les flics peuvent bénéficier de moyens plus importants. Toutefois le procès n'ayant pas encore eu lieu, il nous semble prudent de ne pas tirer trop de conséquences et de liens hâtifs entre la manière dont cette histoire a été instruite et le fait qu'elle soit sous juridiction antiterroriste.

Nous allons maintenant essayer de résumer tous les différents types d'actes que la justice et la police enclenchent lors d'une enquête, en s'arrêtant un peu plus sur certains aspects techniques.

Exploitation d'un téléphone portable

Voici des extraits du rapport concernant les méthodes d'expertises d'un téléphone portable (qu'on appelle parfois GSM dans ce texte) à destination des juges et des parties. Il n'y a pas de véritable scoop dans cet extrait, ça confirme, clarifie et donne une petite idée du résultat et de tout ce que permet l'exploitation d'un téléphone portable. On remarque qu'il est presque possible d'avoir autant d'infos sans avoir le téléphone ou la puce entre les mains, juste en sollicitant l'opérateur, et que l'étendue des infos obtenues est importante. On voit par exemple qu'il est possible d'établir des corrélations à distance entre téléphone et carte SIM, de savoir dans quels téléphones et combien de fois a été utilisée une carte SIM. C'est donc bien insuffisant de changer de carte SIM si l'on conserve le même téléphone (bien que l'expertise dans l'autre sens n'apparaisse pas explicitement, c'est-à-dire partir du téléphone et en déduire les cartes SIM utilisées dedans). On note aussi les fichiers de plusieurs dizaines de noms avec une fiche pour chacun en partant des numéros les plus en communication avec une carte SIM expertisée à distance.

Il existe de plus grâce aux téléphones toutes les possibilités de géolocalisation, en direct ou a posteriori, et les possibilités d'en faire des micros d'ambiance, ce qui n'apparaît pas dans notre dossier. Autant de bonnes raisons de bien réfléchir à l'utilisation qu'on fait d'un téléphone portable.

« **Expertise d'une carte SIM saisie :**

Pour procéder à l'expertise de la carte SIM, nous avons utilisé un lecteur pour cartes à puces de marque GEMPLUS et un logiciel d'analyse « GSMView ». L'analyse des données contenues dans la carte à puce est réalisée sans connexion au réseau, évitant ainsi toute modification interne des mémoires. C'est pourquoi l'analyse de la carte à puce est toujours entreprise avant celle du téléphone. L'extraction des données contenues dans le portable est donc effectuée après que celle de la carte à puce ait été sauvegardée et retranscrite dans le rapport.

Sans risques d'altérer les données, le logiciel « GSMView » lit les éléments suivants : le nom et le pays de l'opérateur ayant délivré la carte / le numéro de série de la carte (ICCID) / 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 ».

Ce matériel d'analyse des mémoires de cartes à puce permet ainsi d'accéder à des données utilisées par l'opérateur et par le matériel de communication, données auxquelles l'abonné n'a pas accès. C'est le cas du numéro IMSI qui est l'identifiant unique de la carte

Juges d'instruction du pôle antiterroriste du Tribunal de Grande Instance de Paris, la galerie Saint-Eloi : Marie-Antoinette Houyvet / Edmond Brunaud.

Expert judiciaire en empreintes génétiques : Sandrine Valade

Quelques exemples d'observations de rassemblements

Il s'agit de la manifestation du 5 avril 2008 pour la liberté de circulation, peu après les premières arrestations et incarcérations dans cette affaire, et le rassemblement au tribunal de Paris le 28 avril en solidarité avec les personnes incarcérées.

Lors de ces évènements la SDAT est sur place et tente de recueillir des infos en collaboration avec les RG. Sur la manif du 5 avril, les RG disent reconnaître une dizaine de personnes dans le cortège ciblé. Leurs noms ainsi qu'une rapide fiche de renseignement figurent au dossier. La SDAT prend 180 photos et en tire 200 portraits (avec donc une dizaine de personnes identifiées) pour réactualiser son « Album photo évolutif ». Ces photos serviront notamment lors d'enquêtes de voisinage concernant certains lieux.

Au tribunal le 28 avril, la SDAT identifie 22 personnes sur les 70 présentes mais il faut noter qu'il y a eu des contrôles d'identité ce jour-là, on ne sait pas quelles identités proviennent de ces contrôles et lesquelles de leurs renseignements ou de leurs copains RG. Ils prennent pleins de photos et en tirent 70 portraits qu'ils relient aux 22 personnes identifiées.

L'analyse des empreintes génétiques

Cet extrait concerne le document que les experts transmettent au juge pour expliquer la démarche du relevé des empreintes génétiques. Des brochures sont récemment sorties sur ce sujet et cet extrait n'apporte pas beaucoup de nouvelles infos. L'extrait est parfois écrit dans un langage ardu, nous avons tenté de surligner quelques passages pour en favoriser la lecture :

« *Empreintes génétiques – Expertise – Annexe :* ***Typage ADN Mitochondrial***

Principe : L'ADN nucléaire, qui présente une grande variabilité d'individu à individu, n'existe qu'à un seul exemplaire par cellule. Un autre ADN, situé dans les mitochondries, est présent à plusieurs centaines d'exemplaires dans la cellule. De ce fait, l'analyse de cet ADN mito-

leurs renseignements pour avoir participer à tel collectif dirigé par Y, pour participer à des collages nocturnes et qu'il était présent à l'expulsion mouvementée du lieu squatté ….. (sans qu'il n'y ait eu de contrôles d'identité à ces occasions). »

Voici un exemple d'une fiche du Fichier des personnes Recherchées (FPR) transmise au dossier :

L'élément le plus intéressant de cette fiche est qu'ils écrivent qu'en cas de contrôle d'identité, il convient de ne pas attirer l'attention de la personne contrôlée pour des motifs de sûreté de l'État tout en avisant les Renseignements Généraux de la préfecture de Police de Paris du contrôle d'identité.

« *Ministère de l'intérieur.*

Fiche confidentielle pour les autorités judiciaires, de police, de gendarmerie et administratives dans le cadre de leurs compétences.

Identité principale : Identité : nom / prénom / né le ….. à ….. Nationalité :

Informations générales : Mesure immédiate : ***ne pas attirer l'attention***
Motif : sûreté de l'Etat
Sommaire : 1 identité, 1 fiche

Fiche active :
Renseignements Généraux n°…..
Sûreté de l'Etat Mesure immédiate : ***ne pas attirer l'attention***

Motif : Individu proche de la mouvance anarcho-autonome susceptible de se livrer à des actions violentes

Service demandeur : Préfecture de police Renseignements Généraux Paris – Tél : 0153733815

Conduite à tenir : SO4 – ***en cas de découverte aviser les RGPP*** »

Quelques noms de flics, de juges et d'experts qui se sont occupés de cette affaire

Sous-Direction Anti-Terroriste (SDAT) de la Direction Centrale de la Police Judiciaire (DCPJ), ceux de Levallois : Arnaud Lambert (Capitaine) / Stéphanie Suchon / Joël Dugourd / Cyril Mulat / Laure Dominguez / Selim Hamadache / Jérôme Wellart-Crépin / Bruno Mancheron

Brigade Criminelle de la Préfecture de Police de Paris, Section Anti-Terroriste, 36 quai des Orfèvres : Mario Menara (Commandant) / Julien Mabrut / Christophe Boucharin / Christophe Paugoy / Dominique Wieczorek / Tristan Ratel / Daniel Terrasse / Loïc Garnier / Philippe Lamaud.

SIM et qui permet à l'opérateur de déterminer le compte de l'abonné.

Remarque sur le numéro IMSI : Le numéro IMSI correspond au numéro de série international de la carte SIM, c'est le numéro d'identification unique de la carte SIM. Il permet d'identifier l'utilisateur sur le réseau de téléphonie mobile et de déterminer le pays et l'opérateur correspondant à l'abonnement de cette puce. Il permet aussi d'identifier le client sur le compte duquel les communications téléphoniques sont débitées (si la carte n'est pas une carte rechargeable). Ce n'est pas forcément l'acquéreur du mobile. Une carte SIM peut, en effet, être utilisée sur différents mobiles.

A partir du numéro IMSI, différents renseignements peuvent être demandés à l'opérateur de la carte concernée : identité du propriétaire de la carte / numéros appelés, numéros appelants / Stations de base utilisées pendant les communications, cela permet de localiser l'utilisateur avec plus ou moins de précisions (cela dépend de la surface couverte par la station de base)

Expertise d'un téléphone saisi :

Pour procéder à l'expertise de l'appareil, nous avons utilisé une connexion entre le téléphone et un ordinateur dédié. Selon les caractéristiques du téléphone sera utilisé un câble data, une liaison radio (bluetooth) ou une liaison par infrarouge. Nous avons également uti-lisé un logiciel d'analyse des mémoires de téléphone, tel que « XRY », « Oxygen Forensic » ou « MOBILedit » ou un système de lecture spécifique du fabricant de mobile. Les données accessibles extraites sont les suivantes : le numéro d'identification IMEI / les messages écrits reçus, composés et non effacés par l'utilisateur / le ou les derniers numéros émis, reçus et restés sans réponse / les compteurs d'appels (durée du dernier appel, de tous les appels émis…) / le message d'accueil à l'allumage du téléphone / le répertoire téléphonique / les fichiers multimedias (photos, vidéos…) / autres…

Ces informations ne sont pas accessibles sur tous les mobiles. Il existe en effet des modèles plus ou moins élaborés qui permettent l'obtention que d'une partie de ces informations. L'accès à certaines données est subordonné à la présence de la carte SIM d'origine (si le mobile en possède une). Sinon, nous utilisons une carte à puce de test du service, dont la mémoire est préalablement vidée de toute information susceptible d'affecter celle du portable analysé.

Remarque : le numéro IMEI est le numéro d'identification unique du mobile. A partir de ce numéro il est donc possible d'obtenir auprès du fabricant du radiotéléphone l'identité de l'acheteur ou celle du revendeur qui a vendu cet appareil. On peut également savoir si ce mobile a été volé. ***Il est possible d'identifier auprès des opérateurs le numéro des cartes SIM***

utilisées dans un radiotéléphone dont on connaît le numéro IMEI et d'avoir ainsi les renseignements concernant les cartes SIM.

Expertise de la carte d'extension mémoire saisie (c'est la carte qui permet les applications multimedia du GSM) :

Pour procéder à l'expertise de ce support, nous avons utilisé un dispositif de protection contre l'écriture (société Tableau ou Logicube) qui protège les mémoires contre toutes modifications (effacement, altération, formatage) des données présentes dans celle-ci. Tout comme la carte à puce, la carte d'extension mémoire est analysée séparément. L'analyse de la carte d'extension mémoire permet de connaître l'organisation et la taille de chaque fichier utilisé ainsi que la présence d'un système d'exploitation.

Les données accessibles sont les « données apparentes », les « données supprimées » (ce sont celles effacées par l'utilisateur mais existantes encore dans les mémoires de la carte. Il s'agit d'éléments ayant le statut de « fichier supprimé ». En l'espèce, ils ne s'affichent plus à l'écran du portable et de l'ordinateur. Il est à noter que certains fichiers supprimés ont été dégradés et ne peuvent plus être restaurés dans leur intégralité) et les « données brutes » (ce sont les fichiers reconstitués à partir des données présentes dans la mémoire du support et révélés à partir de leur signature. Le nom, la taille et la date d'enregistrement ne peuvent être précisés).

Expertise de la messagerie vocale du téléphone :

Pour sauvegarder le contenu de la messagerie, il convient à partir d'un téléphone filaire du service de joindre, selon la procédure de l'opérateur, le centre de messagerie de l'abonné et de procéder à un enregistrement direct par la liaison filaire des messages reçus et archivés. Il est à noter que les trois principaux opérateurs français peuvent effacer volontairement des messages vocaux pour éviter de saturer leurs équipements.

Contacts pris avec les services techniques des opérateurs, il nous a été précisé pour ce qui concerne les délais de conservation : Chez SFR : un message vocal est conservé une semaine après son enregistrement sur le serveur si l'abonné l'écoute. Sinon il s'efface après 48 heures / Chez Orange : Ecouté ou non le message s'efface après une semaine à partir de son dépôt en messagerie vocale / Chez Bouygues Télécom : Le délai de conservation d'un message vocal est de deux mois s'il n'est pas consulté par l'abonné. Après lecture il s'efface après 48 heures. Il peut toutefois être sauvegardé pour une période d'un an pour une somme modique. »

Exploitation d'une ligne (sans avoir ni le téléphone ni la carte SIM entre les mains) :

« *Selon les renseignements collectés, il semble vraisemblable que Z utilise le numéro de mobile 06….. Indiquons et à l'insurrection ont été lancés. Des incidents se sont produits place de la Bastille et aux alentours le soir du second tour et les soirs suivants.*

La semaine de solidarité de juin 2008 a été le point d'orgue des actions de solidarité de la mouvance. Cette semaine a démontré la détermination des individus composant cette mouvance, visant avec discernement des cibles engagées. Les actions à l'étranger démontrent l'existence de relations étroites, internationales et anciennes des individus de cette mouvance, grâce à Internet. Le degré de gravité des actions est relativement faible mais soulignons qu'elles sont coordonnées, ce qui démontre l'existence d'un réseau capable de déclencher des actions simultanées sur un thème identique et de centraliser les revendications. »

Exemple de fiches de renseignements jointes au dossier

Encore une fois prudence avec ce genre d'informations, ce sont quelques exemples dont nous avons eu connaissance, ce ne sont pas des généra-lités, et les quelques renseignements transmis par les flics dans les dossiers judiciaires ne signifient pas qu'ils n'ont pas d'autres infos qu'ils ne transmettent pas. Nous avons d'ailleurs remarqué différents niveaux de renseignements communiqués dans leurs « fiches de renseignements » sur X ou sur Y qui figurent dans les dossiers judiciaires.

Il y a des fiches de renseignements de base avec les infos suivantes : état civil détaillé (nom, prénom, date de naissance, lieu de naissance, nom des parents), domicile connu, permis de conduire, voiture détenue, numéro des papiers d'identité détenus. A cela et selon les exemples peuvent s'ajouter d'autres infos : photos (d'une garde à vue précédente ou du fichier des cartes d'identité), revenus déclarés, emplois connus ou pas des services de police, éventuel fichage aux renseignements généraux (Fichier des personnes recherchées – FPR –, fiche aux RGPP – RG de Paris –, fiche à la feu DCRG – les ex-autres RG – de-venus la DCRI), fichage au STIC (Système de Traitement des Infractions Constatées), c'est-à-dire le récapitulatif des gardes à vue et des contrôles d'identité et des personnes avec qui l'intéressé a été contrôlé (heureusement leurs systèmes sont loin d'être infaillibles et souvent il manque des trucs).

Enfin il y a eu dans quelques cas des infos « de première main » qui ne sont liés à aucun contrôle d'identité ni rien, juste du renseignement du type « *Les services spécialisés de la région de ….. nous signalent que l'individu X y a séjourné et qu'il y était connu selon*

type de mélange est d'ailleurs souvent utilisé dans la réalisation de « Pipe Bombs ». L'initiation de ce type de mélange s'effectue de manière simple avec une mèche enflammée. Un essai de brûlage a été réalisé au laboratoire central. Le mélange s'enflamme difficilement à la flamme nue. Ceci explique la présence d'allume-feu pour initier. »

Quelques renseignements concernant la mouvance anarcho-autonome francilienne et la semaine de solidarité de juin 2008

« *Février 2008 : On peut estimer le noyau de cette mouvance à une cinquantaine d'individus âgés de 20 à 30 ans, d'origine européenne pour la quasi-totalité, auxquelles s'agrègent selon les circonstances 150 à 200 personnes, membres de diverses organisations libertaires. Leur thème fédérateur est* « la haine de l'Etat bourgeois, du capitalisme et de ses appareils ». *Ce rejet s'exprime par des actions concertées à l'encontre des forces de l'ordre et des symboles du capitalisme (banques, agences d'intérim, compagnies d'assurances, sociétés commerciales internationales…) préparées par les intéressés lors de rencontres dans des squats, à la fois lieux de vie, de réunion et de passage. Depuis début 2007 on constate en Ile-de-France une radicalisation de la mouvance anarcho-autonome francilienne. Deux raisons expliquent cette évolution : l'apparition d'une nouvelle génération née du conflit anti-CPE de 2006, et le contexte électoral, un certain nombre de ces jeunes ayant éprouvé une véritable aversion à l'encontre du candidat de l'UMP. La campagne a en effet été marquée par un certain nombre d'actes imputables à la mouvance anarcho-autonome francilienne. Des dégradations de permanences de partis politiques à Paris (21 de l'UMP ont notamment été visées) revendiquées par voie d'affichage* « une façon comme une autre d'exprimer son refus de la politique institutionnelle, une façon bien plus claire en tout cas que d'aller mettre un bulletin dans une urne ». *Le 2 mai, un engin incendiaire artisanal a été découvert sous un véhicule d'enlèvement de la police à proximité du commissariat de la rue de Clignancourt. Des incendies de véhicules revendiqués également par voie d'affichage :* « Cramer des voitures aura toujours plus d'impact politique que de mettre un bulletin dans une urne. Vive le feu ! ». *27 ont ainsi été commis dans la nuit du 5 au 6 mai, nuit précédant le second tour. De plus, dans la perspective du soir du second tour de l'élection présidentielle, de nombreux appels à l'émeute*

avoir requis l'opérateur téléphonique Bouygues (ou Orange, ou SFR) afin qu'il nous communique l'ensemble des renseignements en sa possession concernant le n° 06….. , ainsi que la facturation détaillée et la localisation des bornes activées de ce numéro pour la période s'étalant du … au …. (c'est-à-dire la dernière année écoulée) » Suite à une réquisition auprès de l'opérateur (qui coopère en quelques heures ou quelques jours), il est écrit : « *le numéro de téléphone 06….. est attribué à Z, né le …, titulaire de la carte nationale d'identité n°….. , élisant domicile au ……. à …… . Il a déclaré également un numéro de téléphone fixe auprès de l'opérateur Bouygues, il s'agit du numéro 01…... Il a fourni lors de l'abonnement les coordonnées bancaires suivantes …… la ligne a été mise en service le ….. , suspendue le …… pour vol puis réactivée le …..* ». Toutes les informations sont donc données lors de la souscription à l'abonnement dans l'agence de l'opérateur figurent : état-civil / adresse postale / adresse mail / date de la souscription / type et numéro de la pièce d'identité fournis lors de la souscription / moyen de paiement utilisé et coordonnées bancaires si paiement par virement / IP en cas de numéro Freebox par exemple.

Exemple de l'étude d'une ligne sur un an : « *Le numéro 06….. a fait transiter 4101 appels durant cette période. Les numéros appelés et reçus sont, dans l'ordre décroissant : le numéro 06….. , 817 appels, attribué à Y.* » S'ensuit une fiche sur Y avec tous les renseignements comme précédemment cités, éventuellement accompagnés d'une fiche de renseignements type RG, assez succincte dans notre exemple (« *Y est un militant connu depuis de nombreuses années, habitant les squats de la région parisienne…* »). Puis le numéro 06….. , 641 appels, attribué à X… et ainsi de suite. La liste dans notre exemple comporte ainsi plus d'une cinquantaine de noms, avec pour chacun plus ou moins de renseignements, au minimum un petit état civil, nom, prénom, date de naissance, adresse. Cette énumération est également accompagnée de commentaires du type : « *Nous signalons que le numéro 06….. , attribué à P, est déjà apparu dans cette procédure dans le répertoire de N…* », mais ce n'est absolument pas systématique.

Ce type d'étude à distance permet aussi de faire des liens entre des téléphones et des puces utilisées, des associations entre les numéros IMEI (boîtiers) et IMSI (puces). Par exemple concernant X, il est écrit : « *Le numéro de boîtier ….. a permis de faire transiter 1337 communications par le biais de la puce 06….., attribuée à X. Cette puce a été introduite à ….. reprises dans le boîtier n°….. , à 417 reprises dans le boîtier numéro ….. , à 44 reprises dans le boîtier numéro …..* » et ainsi de suite. Tout ça sans jamais avoir eu le téléphone ni la puce entre les mains.

Les écoutes téléphoniques

Les flics (Julien Mabrut en l'occurrence) s'adressent à l'opérateur Bouygues Télécom pour intercepter et enregistrer les communications transitant par le numéro 06….. , attribué à X. Ils s'adressent au : Services des Obligations Légales – Lutétia V – 15/17 rue du Colonel Pierre Avia – 75729 Paris. Ils demandent également à Bouygues un rapport technique quotidien à envoyer à l'adresse : julien.mabrut@interieur.gouv.fr. Ce sont ainsi 800 appels en 3 mois qui seront interceptés, seules figurent au dossier une dizaine de conversations considérées comme les plus intéressantes.

Les flics mettent en place pendant 24 heures un système de géolocalisation en temps réel (Loc TR dans leur jargon) pour essayer de trouver une personne recherchée. Il est à noter que cette géolocalisation concerne des téléphones des proches de la personne recherchée et non le téléphone de la personne recherchée elle-même. Avoir son téléphone sur soi implique donc plus que juste pour sa propre sécurité. La procédure pour la géolocalisation en temps réel est identique à celle pour des écoutes et passe par l'opérateur qui transmet les données. Il y a dans le dossier un certain Benoit Gosse de la société Deveryware qui semble proposer des services très performants en matière de géolocalisation en temps réel, il laisse même son numéro : 06.70.27.71.44.

Renseignements sur un site web

Enquête sur l'origine d'un article de revendication de l'incendie d'une agence BNP à Paris le 3 juillet 2008, paru sur le site « NANTES.INDYMEDIA.ORG ». Cet incendie fait l'objet d'une enquête préliminaire de la Brigade Criminelle de la Préfecture de Police de Paris (n°257/2008).

Renseignements sur le site :

« Acheteur du nom de domaine et de l'administrateur du site : Société ….. , rue ….., SAO PAULO (BRESIL) Hébergeur du site : ….. , société créée par ….. , domiciliée ….. SEATTLE (USA). Seul un cadre juridique approprié permettrait de requérir ces deux sociétés basées à l'étranger pour avoir les connexions IP. Toutefois il apparait que le site « Indymedia.org » est aussi hébergé temporairement sur ….. , de tendance anarcho-autonome. ….. a été enregistré auprès du fournisseur d'accès français ….. avec les coordonnées suivantes : ….. Paris. Les recherches ont établi que cette société est fictive. Le site ….. est hébergé auprès d'un fournisseur d'accès US, ….. domicilié à Seattle. La date de création de ce site est trop ancienne pour pouvoir remonter sur la transaction bancaire ayant permis de l'enregistrer auprès de ….. . » Suite à la "semaine de solidarité" en juin 2008, des recherches ont lieu sur des actes et sur leurs revendications sur des sites Indymedia. A cette occasion les flics écrivent : « *Précisons que les serveurs hébergeant les sites du réseau Indymedia, domiciliés aux USA à Seattle, refusent systématiquement de donner connaissance aux autorités des logs de connexion des ordinateurs consultant ces sites ou y déposant une contribution, rendant de fait non-identifiable les auteurs des contributions, tels le ou les rédacteurs du communiqué sui-vant : "Chronologie de la semaine de solidarité"* ».

Renseignements bancaires

Après s'être adressée à la DRESG (Direction des Résidents à l'Etranger et des Services Généraux), cette enquête permet d'obtenir des renseignements fiscaux et bancaires : comptes bancaires (fichier Ficoba – Fichier national des comptes bancaires et assimilés), éléments « Adonis » (adresse, situation familiale, bulletins de recoupements des salaires…), situation fiscale. Ensuite une réquisition auprès d'une banque où l'intéressé a un compte permet d'avoir le détail de toutes les activités du compte.

Expertise technique concernant la composition d'un fumigène

Voici pour l'anecdote une petite recette qu'ils nous transmettent pour bien doser un fumigène (un tiers de chlorate, un tiers de sucre, un tiers de farine) ou autre : « *Le chlorate de soude est souvent utilisé par les artificiers amateurs pour réaliser des compositions explosives ou incendiaires. Dans le cas présent, le dosage semi-quantitatif effectué au laboratoire central montre que du chlorate de soude, conforme à l'avis du ministère de l'agriculture, de la pêche et des affaires rurales, a été utilisé. En effet il contient deux substances pour abaisser la concentration en chlorate, le chlorure et le bicarbonate de sodium. Dans ce cas il avait été rajouté des combustibles (saccharose et farine) en proportion beaucoup trop importante. En fait, le mélange explosif, qui déflagre notamment sous l'effet d'une flamme est de l'ordre de 55% de chlorate de soude pour 45% de sucre. Dans le cas présent, il y a un important déficit en oxydant. Ce*