

**Pour Coulisses médiatiques
Philippe Madelin**

Décembre 2007

Des « zonzons », des constructions et des hommes

Écoutes et interceptions :

De la curiosité mal placée ? De la prévention du terrorisme ? De l'enquête judiciaire ?

Ça commence toujours de la même manière, par cette réflexion :

- J'entends des bruits bizarres dans mon téléphone, ce sont les écoutes. On m'écoute.

Il y a belle lurette qu'on ne peut plus savoir si on est écouté par un service officiel quelconque. Depuis l'époque où j'ai pu voir au central téléphonique « Tuileries » ou à la Section de recherche de la Gendarmerie à Ajaccio des batteries de magnétophones enregistrant des conversations téléphoniques les techniques ont évolué de façon prodigieuse. Aujourd'hui assurées par des instruments très sophistiqués, les interceptions, c'est le terme consacré, sont non seulement indétectables, mais, bien sûr, nulle « cible » n'est avertie de leur mise en place. Et pour cause : si on sait, on ne dit plus rien. Le secret de l'écoute est un facteur décisif. Et tout à fait légal, contrairement à une opinion répandue. On estime que chaque année plusieurs dizaines de milliers de « constructions » - ou branchements - sont mis en place. En outre, désormais tous les moyens de communication sont susceptibles d'être écoutés ou enregistrés : le téléphone fixe, le téléphone cellulaire, les messageries internet, en bref tout notre environnement cybernétique. Et des logiciels spécialisés permettent de repérer les messages « inopportuns » à partir de mots-clé pertinents.

Une légalité à deux vitesses.

En réalité on distingue au moins deux catégories d'écoutes. d'une part les interceptions dites « judiciaires », découlant de commissions rogatoires émises par les juges d'instruction. Leur transcription est versée au dossier d'enquête judiciaire – enquête préliminaire ou instruction - .

Dans une récente interview (<http://www.bakchich.info/article2105.html>, 22 décembre 2007) l'écrivain Denis Robert proteste vivement contre sa mise sous écoute. Juridiquement il a tort : comme il a été mis en examen dans le dossier Clearstream, les juges Pons et d'Huy ont décidé de placer sous surveillance Robert et tout son entourage, en vue de recueillir des éléments pour leur dossier. En vertu du principe du débat contradictoire, ces transcriptions doivent d'ailleurs être communiquées aux intéressés.

Moins évidentes, mais non moins légales sont les écoutes dites « administratives », ou « interceptions de sécurité », visant le recueil du renseignement. Cette question a été l'objet de longs et larges débats lors de l'affaire dite des « Écoutes de l'Élysée » et au cours du procès qui a suivi en février et en septembre 2005. Rappelons les faits : dans les années 1986-1988, une cellule de renseignement spéciale avait été installée auprès de la Présidence de la République, en principe pour prévenir le terrorisme, en pratique en partie pour surveiller les personnes s'intéressant de trop près à Mazarine Pingot, fille du Président François Mitterrand.

Police anti-terroriste : l'interception des données entre dans une nouvelle phase

L'acronyme américain SIGINT s'applique à toutes les communications transitant par voie électronique.

En France leur interception entre dans une phase absolument nouvelle, sinon révolutionnaire : les procédures judiciaires et techniques sont désormais au point, les structures bientôt toutes en place. La loi du 23 janvier 2006 légalise cette nouvelle construction.

Une fois n'est pas coutume : les éléments d'information sont assez largement diffusés, et cette diffusion est clairement dans les programmes de prévention et de lutte contre le terrorisme. Voire de

dissuasion : il est signifié aux « malfaisants » que désormais toutes leurs connexions téléphoniques ou informatiques peuvent être identifiées et localisées très vite.

Nous appellerons Yannis ce jeune Français de souche « converti » à l'islam. Des policiers appartenant aux Renseignements Généraux, en poste en Seine-Saint-Denis l'ont repéré parmi les pratiquants assidus d'une salle de prière de Clichy-sous-Bois. Le jeune homme est devenu un risque, il présente un certain nombre de signes qui permettent de le considérer comme potentiellement suspect, sans qu'aucun délit ne puisse lui être reproché : il téléphone beaucoup, il fréquente assidûment des cybercafés : pour jouer, ou dans un autre but. Récemment on l'a vu dans un parc tapoter sur son ordinateur portable, probablement connecté à une borne WiFi.

Jusqu'à ce mois de mai, sans compter les équipes de policiers chargées de le suivre, la surveillance rapprochée d'un tel « personnage » nécessitait un dispositif lourd et coûteux, centré autour de la mise sous écoute de ses différents moyens de communication : téléphone fixe et portable, ligne informatique, etc. Des semaines étaient parfois nécessaires pour que tout soit mis en place après autorisation formelle donnée par la CNCIS – Commission de contrôle des interceptions de Sécurité -, au prix d'un investissement considérable, plusieurs dizaines de milliers d'euros pour un résultat aléatoire.

Depuis le 2 mai, le système est totalement modifié.

Désormais au sein du service chargé de détecter les risques, ici la section 93 des RGPP, pour entrer dans le processus, un fonctionnaire habilité passe un simple message – crypté – à la nouvelle plateforme technique d'interception des données de connexion aux systèmes de communication gérée par l'UCLAT (Unité de coordination de la Lutte antiterroriste) et installée dans les nouveaux locaux du Ministère de l'Intérieur à Levallois. Contenu du message : demande d'autorisation pour placer sous surveillance les communications passées par Yannis, l'individu désigné : identification précise de ses téléphones fixes ou mobiles et le ou les adresses IP de ses moyens informatiques ; demande de communication de tous les abonnements liés aux numéros repérés et des documents d'inscription ; relevé précis de toutes les connexions téléphoniques – entrées et sorties - ; destinataire ou émetteur des SMS, dates et heures ; adresses internet personnelles et sites internet consultés, soit par câble, soit par système WIFI ; géolocalisation des connexions par téléphone portable. Le champ d'investigation est large, mais, à ce stade, ne porte pas sur le contenu des communications.

La plateforme est un simple relais technique, en quelque sorte un serveur. Par application de l'article 6, loi du 23 janvier 2006, le serveur bascule la demande sur le service qui, à l'Inspection générale de la Police Nationale qui est légalement investi de l'évaluation. Cette fonction est assurée par l'Inspecteur général François Jaspard et quatre adjoints disponibles jour et nuit.

Trois réponses sont possibles : c'est oui, c'est non, ou bien la demande nécessite des éclaircissements supplémentaires. Après validation par signature électronique infalsifiable, l'Inspection notifie sa décision à l'UCLAT. Celle-ci peut alors saisir tous les opérateurs téléphoniques et/ou informatiques qui sont tenus de communiquer toutes les informations en leur possession. Dernier stade, l'UCLAT retransmet les résultats de l'enquête au service demandeur d'origine, en l'occurrence la section de Seine-Saint-Denis des RGPP.

A première vue, ce système est un peu lourd. En pratique, il ne prend que quelques heures, à opposer aux délais considérables nécessaires pour que la CNCIS.

Curieusement c'est selon François Jaspard une protection supplémentaire des libertés publiques puisque toutes les demandes doivent être instruites et autorisées avant mise en œuvre.

Toutefois les informations ne peuvent concerner que les données techniques des connexions, il ne s'agit pas d'une écoute au sens strict. En quelques sorte, il s'agit d'un tri préalable : dans notre

exemple, il peut parfaitement se trouver que les communications passées par Yannis ne présentent aucun caractère suspect, malgré l'apparence initiale.

En revanche, si les suspicions à l'encontre de la cible subsistent, le service a la faculté de demander à la CNCIS une écoute à caractère administratif en bonne et due forme. L'interception portera cette fois-ci sur le contenu des conversations et des messages, on se retrouve dans le schéma antérieur au 2 mai.

Mais nous restons là au niveau de la recherche du renseignement.

Un dernier stade est cependant possible, au niveau judiciaire, désormais : admettons qu'il soit établi par les écoutes et tout autre moyen que le dénommé Yannis est suspecté de participer à une action à caractère terroriste. Menées dans le cadre strict de la procédure pénale, l'enquête préliminaire ou l'instruction doivent déterminer la nature et l'ampleur des infractions commises. Le procureur chargé du dossier et/ou le juge d'instruction peuvent alors demander la mise en place d'écoutes à caractère judiciaire, dont ils assureront le contrôle ; le compte-rendu apparaîtra dans le dossier judiciaire comme des pièces à conviction, ce qui n'est pas le cas des interceptions et écoutes administratives, qui ne relèvent que du renseignement à caractère préventif.

Sur un plan pratique

Les services de police habilités à demander des autorisations et uniquement dans le cadre de la lutte anti-terroriste sont : la Direction Centrale de la Police judiciaire, la Direction centrale des Renseignements généraux, la DST, la Direction générale de la Gendarmerie nationale, les Renseignements généraux de la Préfecture de police, la PJ de la Préfecture de police et l'UCLAT.

Au 25 mai 2007 1130 demandes de « mise sous surveillance électronique » avaient été autorisées par l'Inspection générale de la Police nationale.

Par ailleurs, la Direction générale de la Police nationale a confié à François Jaspard une mission de réflexion sur l'impact des nouvelles techniques de l'information sur les techniques de police. En termes plus administratifs : la cybercriminalité et l'usage frauduleux des techniques de l'information, vers une police technologique.