UNIVERSITÉ PANTHÉON-ASSAS (PARIS II) - **INSTITUT DE CRIMINOLOGIE DE PARIS**

DÉPARTEMENT DE RECHERCHE SUR LES MENACES CRIMINELLES CONTEMPORAINES

DÉPARTEMENT MCC - BUREAU 507 • 28 RUE SAINT-GUILLAUME • 75007 PARIS

Actes du colloque

«Écoutes et interceptions légales des télécommunications

Les nouveaux enjeux technologiques et financiers»

Sénat 5 octobre 2006

Sous le haut patronage de Christian Poncelet, Président du Sénat
Sous la présidence du Sénateur Jean-Jacques Hyest, Président de la Commission des Lois

Présentation par François Haut, directeur du DRMCC

(Département de Recherche sur les Menaces Criminelles Contemporaines, Institut de Criminologie, Université PARIS II Panthéon Assas)

François Haut, directeur du DRMCC après avoir remercié le Sénat pour son accueil et avant de passer la parole à François-Bernard Huyghe qui présentera le rapport, rappelle les activités du DRMCC de l'Institut de Criminologie rattaché à l'Université Paris II et créé en 1997.
Ses principaux points d'intérêt sont l'étude des nouvelles formes du crime organisé et du terrorisme, voire la fusion des deux après la chute du Mur, notamment à travers le phénomène des « guérillas dégénérées ».

Il rappelle également la méthode du DRMC : le décèlement précoce des nouveaux phénomènes criminels, donc la détection des signaux faibles (une activité qui a nourri les nombreuses notes d'alerte émises par le département depuis quatre ans).
Nombre de sujets furent ainsi abordés : l'implantation des mafias albanaises en Europe occidentale en 2000-2002, l'arrivée massive de la cocaïne, dont on découvre officiellement la réalité aujourd'hui, les gangs de prison (voir les événements de Sao Paulo 2006), Les fausses identités, le crime organisé russe, les gangs de motards criminalisés. Également parmi les thèmes de colloques et de rapports : les vols de voiture et équipements de traçage, les attaques de fourgons blindés et le marquage des billets, les machines à sous clandestines et la guerre criminelle induite……

Quant au sujet du jour, les interceptions, François Haut rappelle qu'il a fallu que ce soit la Cour européenne des Droits de l'Homme qui en fixe le cadre pour que leur légitimité soit admise et qu'elles soient correctement mises en oeuvre.

Aujourd'hui, la place des interceptions dans la réponse aux menaces - potentielle quand il s'agit de terrorisme et présumée quand il s'agit de crime organisé - et la diversification des techniques de communication, sont de nouveau défis pour cette violation légale du secret de la correspondance.

Il était donc utile de réfléchir à la rationalisation des interceptions légales aux fins de les rendre plus fiables, plus utiles, plus précises, plus efficaces, mieux contrôlées et moins coûteuses.

Raison de plus de produire un rapport avant que les passions s'enflamment à nouveau et que le débat soit faussé par des polémiques obscurcissant la vraie nature de la question.

Écoutes et interceptions légales des télécommunications

Présentation du rapport par François-Bernard Huyghe

http://www.huyghe.fr/actu_269.htm

La justice transalpine vient de découvrir un système d'écoutes illégales au sein de Telecom Italia. Il fonctionnait depuis 1997 en relation avec une agence de détectives et touchait des milliers de gens dans le monde de la politique, du sport, du spectacle ou des affaires. Ce scandale s'est traduit par de nombreuses arrestations et par le suicide «à la Stavisky» d'un responsable de la sécurité de Telecom. Et cela au moment où nos voisins s'apprêtent à voter la loi Mastella sur les interceptions de télécommunications afin de mieux maîtriser la technique, le nombre et la gestion des écoutes judiciaires. Or celles-ci se sont multipliées de façon spectaculaire surtout dans le cadre des enquêtes menées contre la Mafia.

En Grèce, le monde politique bruit encore de la découverte d'un logiciel espion, sans doute implanté par une agence de renseignement étrangère il permettait d'écouter les téléphones mobiles de ministres ou autres personnalités.

Aux Etats-Unis, il ne se passe pas de semaine où la presse ne revienne sur les écoutes illégales de milliers de citoyens dans le cadre de la lutte contre le terrorisme. Des associations de citoyens et des juristes contestent aux autorités le droit d'intercepter des conversations avec l'étranger sans mandat (même d'une « cour secrète » comme il en existe outre-Atlantique pour certaines affaires particulièrement sensibles). La question des libertés publiques et de la surveillance électronique sera au cœur du débat sur les élections du prochain *mid-term*.

Au-delà de la question politique

Que déduire de ce qui précède ou de dizaines d'autres exemples que nous pourrions puiser sous d'autres cieux ? Que nous sommes tous espionnés? Que Big Brother a gagné ? Que la France, un moment secouée par le scandale des écoutes de l'Elysée, est devenue un havre de démocratie dans un monde où chacun est intercepté, fiché ? Que le seul problème chez nous est que les interceptions coûtent trop cher au Ministère de la Justice ?

La réponse est : non. Ce n'est pas rendre service à la cause des libertés (sans parler de celle de la répression du crime qu'il est usuel d'opposer à la première) que de tout mettre sur le même plan.
- Le légal et l'illégal.
- -Les gigantesques systèmes d'interceptions dont celui de la National Security Agency (un budget supérieur à celui de la CIA, des millions de communications interceptées par jour, le fameux réseau Echelon…) et nos gendarmes écoutant des truands, les écouteurs sur les oreilles.
- Les vieilles et les nouvelles technologies.
- La stratégie que nous nommerons de la nasse (les services de renseignements qui interceptent des millions de communications et les filtrent à la recherche de termes significatifs) ou encore la stratégie du parasite (introduire un logiciel espion dans un téléphone ou un ordinateur) et la méthode légale. Cette dernière consiste à requérir un

opérateur de téléphonie ou fournisseur d'accès Internet de retransmettre une ligne aux enquêteurs ou de leur donner accès à certaines mémoires numériques puis à demander à une société ayant pignon sur rue le matériel et les lignes pour traiter et faire circuler en toute sécurité ces données. Le tout le plus officiellement du monde, avec mandats et procès verbaux, …

La question sensible des « écoutes » est certes d'abord politique : dans quelles conditions les représentants de l'État ont-ils le droit de violer l'intimité de la correspondance électronique entre les citoyens ? Ce débat politique doit s'interprète en fonction d'un double critère sociologie. Celle du crime d'abord : les réseaux criminels ou terroristes eux aussi « travaillent » de façon « nomade », se déplacent, se connectent, échangent et donc au final communiquent de plus en plus. Mais les citoyens ordinaires sont aussi plus sensibles à la question de la surveillance électronique : la peut légitime d'une société de contrôle où chacun serait suivi par les traces numériques que laissent communications, transactions et déplacements dans des bases de données.

Toutes ces interrogations légitimes sont faussées si on ne les pense pas aussi en termes de technologie (ce qui est théoriquement possible) et d'organisation et stratégie (comment on intercepte avec quels moyens et à quel prix ? donc : ce qui se fait pratiquement).

Il va de soi que la technologie des interceptions a évolué autant que celle des télécommunications : c'est la définition de la technologie que de changer. L'indice le plus évident en est la multiplication des terminaux (téléphones mobiles ou ordinateurs). Elle entraîne mécaniquement celle des canaux à intercepter donc celles des interceptions, donc l'augmentation de leur budget.

Encore faut-il mesurer la portée d'une double révolution : celle du numérique (qui réduit tout message à une série de bits informatiques susceptibles d'être transmis, stockés ou traités par diverses sortes de logiciels et d'appareils) et celle de réseaux (qui permettent une connexion de point à point de multiples terminaux).

Les possibilités de la technique

Première conséquence, sémantique: écouter n'est pas intercepter. La «bretelle» posée sur un téléphone filaire comme dans les romans policiers des années 60 permettait d'entendre à distance une conversation de poste à poste, chaque interlocuteur étant repéré par son numéro qui indiquant où il se trouvait (la maison de X, le bureau de Y). Or, nous transmettons désormais en nomades une multitude de données numériques (textes, sons, images) par une pluralité de canaux et en utilisant souvent des identifiants différents, qui sont comme nos clés numériques ouvrant sur le monde des réseaux. Par ailleurs, nous ne communiquons pas que par téléphone : les ordinateurs (ou des appareils mixtes comme les Assistants numériques personnels) servent aussi à transmettre la voix, du courrier électronique, des messageries instantanées, des données son ou image…

Du coup, les enquêteurs ne s'intéressent pas seulement au contenu des conversations ou courriers ; ils recherchent aussi certaines données relatives aux informations : qui a été en communication avec qui, quand et où. Ces informations au second degré (touchant aux conditions de la communication) peuvent renseigner sur la structure d'un réseau criminel ou terroriste et sur l'état de son activité, sans qu'il soit forcément besoin de savoir ce qui se dit.

De plus il est possible de localiser (*géolocaliser* dans le jargon du métier) les appareils téléphoniques mobiles allumés ce qui permet parfois de vérifier un alibi, d'anticiper un flagrant délit, de procéder à une interception… L'intérêt des interceptions ne cesse donc de croître qu'il s'agisse de prévention ou de répression du crime.

Pour autant, faut-il conclure que nos « traces » numériques nous suivent toujours et partout et qu'un système de surveillance électronique permet de reconstituer toutes nos communications ou déplacements comme dans les pires anticipations d'Orwell ? En théorie et en y mettant des moyens illimités, peut-être. En réalité certainement pas.
Il existe des obstacles concrets aux interceptions. Certains résultent simplement de l'évolution des télécommunications :
apparition de nouveaux modes de commutation comme les « chats » ou les SMS, donc apparition de nouveaux protocoles de télécommunications,
prolifération des appareils multifonction (dont ceux qui se connectent sur des réseaux publics notamment par Wifi et qui changent sans cesse de réseau et de point d'accès),
généralisation des techniques dites VOIP (*Voice over Internet Protocol*) qui font passer les conversations en direct par Internet et permettent des connexions de tout point du réseau.

D'autres obstacles résultent des contre-mesures prises par les truands ou terroristes afin de se rendre inécoutables ou non repérables : souvent, ils recourent à des systèmes de chiffrage ou à des leurres (la façon de faire la plus simple est de posséder plusieurs puces pour téléphone). Contrairement à une idée reçue, la technique de surveillance est plutôt en retard et à l'heure où nous parlons « tout» n'est pas *interceptable*. C'est d'autant plus vrai en France où les pouvoirs publics n'ont négocié avec les opérateurs de téléphonie ou fournisseurs d'accès Internet ni les tarifs des interceptions, ni la possibilité technique de les pratiquer sur de nouveaux médias ou canaux. Si on nous autorise ce vilain néologisme, il est urgent de réfléchir à « l'*écoutabilité* » des nouveaux protocoles comme l'ont fait bien d'autres pays. Traduction : la possibilité d'intercepter un nouveau mode de communication chaque fois qu'apparaît soit un nouvel usage d'un appareil (téléphone mobile recevant des SMS ou s'intégrant à certains réseaux d'Internet) soit un nouveau système (comme Skype qui permet de communiquer gratuitement par téléphone via la Toile ou autres systèmes gratuits).

L'organisation des interceptions

Seconde dimension : l'organisation et la stratégie. Restons dans le cadre légal et républicain. Laissons de côté les procédés employés par certains services et officines, et qui sont dignes des gadgets de James Bond. Oublions les logiciels pirates des «hackers ». Cela laisse subsister la question : par quelle procédure, à quel prix et avec quel matériel une autorité peut-elle amener un opérateur à lui retransmettre le contenu de communications « suspectes » et des informations dites « relatives aux interceptions » que gardent leurs ordinateurs (localisation, durée et destination des télécommunications) ? Elle entraîne une question connexe : pour quel usage et sous quel contrôle ?

En France, il existe

- Des écoutes dites administratives ou de sécurité : leur fonction est de déceler en amont des dangers d'une certaine gravité, grand banditisme, terrorisme, espionnage industriel ou autre, et ce à la demande de trois ministères. Ces interceptions sont maintenant contingentées, limitées dans le temps, vérifiées, elles doivent être justifiées, utilisées uniquement si elles sont indispensables quand aucun autre moyen n'est disponible, conformément à une jurisprudence qui s'affirme nettement. Le tout sous le contrôle fort sérieux d'un autorité indépendant où se retrouvent juges et parlementaires la Commission Nationale de Contrôle des Interceptions de Sécurité. Si bien que l'on est passé des « écoutes de l'Elysée » symbole d'arbitraire à un système bien contrôlé et bien accepté.

- Des écoutes dites judiciaires ordonnées par un magistrat instructeur ou un procureur dans le cadre d'affaires d'un type bien défini. Dans la plupart des cas, ces interceptions servent à la manifestation de la vérité pour des crimes et délits pouvant entraîner une peine d'au moins deux aux de prison. Or ces interceptions, pourtant contrôlées par le juge, font l'objet de nombreuses critiques.
-

D'une part, la façon dont elles sont accordées, parfois dans l'urgence, parfois par des magistrats surchargés de travail qui ne peuvent matériellement en vérifier l'opportunité peut donner lieu à des erreurs ou à des abus. Certains parlent même d'écoutes « taxis » : on glisserait dans les listes de numéros dont l'interception est demandée au juge certaines lignes qui n'ont rien à voir avec l'affaire concernée par la procédure judiciaire.

D'autre part ces procédures qui ne cessent de se multiplier (dont le volet «Informations relatives aux interceptions» encore plus onéreux que l'interception «pure» des contenus) coûtent de plus en plus cher. Elles sont payées par le Ministère de la Justice (mais réalisées par les policiers et gendarmes qui dépendent d'autres ministères) et leur coût, comptabilisé dans les frais de justice, contribue pour une bonne partie à leur explosion souvent reprochée.

Certains de problèmes que nous avons évoqués sont en voie de solution : ainsi les tarifs (sans oublier les procédures et les modes de facturation sources des frais inutiles) sont négociés ou en cours de négociation. La fameuse «*écoutabilité*» sera peut-être bientôt à l'ordre du jour.

- D'autres difficultés ressortent à l'organisation administrative et matérielle. Dans le domaine judiciaire, le matériel (les plates-formes d'interception, plus tout l'équipement pour les exploiter en aval) a été choisi dans le désordre, sans mutualisation des matériels ni économies d'échelles. Et souvent en double : police et gendarmerie ayant chacune leur système. Les interceptions sont encore trop souvent installées au coup par coup et entraînent la création d'une ligne spéciale et coûteuse chaque fois. L'existence de plates-formes d'interception qui recevraient des flux numériques, - conversations entre deux mobiles retransmise, données numériques, textes, des images ou des sons, informations relatives aux interceptions – ne signifient pas « régime policier » ou surveillance de tous les citoyens. Au contraire, il est désuet de vouloir faire passer par des moyens ou contrôler par des clefs physiques ce qui est devenu numérique.
-

La traçabilité des systèmes modernes devrait permettre un contrôle a posteriori : qui a eu accès à quoi à quel moment et quelle mémoire en a été conservée. Des centres regroupés à

l'échelle régionale ou inter régionale, avec des procédures de contrôle communes résoudraient une grande partie de ces problèmes (un centre unique « usine à gaz » central n'étant sans doute ni sûr, ni facile à gérer, ni très bien accepté psychologiquement).

- Il serait paradoxal que des officines dotées de matériel espion sophistiqué (comme des «*spywares*», logiciels espions qui s'implantent à distance dans un ordinateur ou un téléphone mobile de troisième génération ou des capteurs pour les ondes émises par les machines à communiquer) puissent tout savoir, tandis que les services officiels agissant sur ordre et sous le contrôle du juge seraient empêtrés par du matériel vieillot ou des méthodes dépassées. En revanche, il ne faut pas que relations dissymétriques entre juges et enquêteurs ou une mauvaise organisation transforme la pratique légale des interceptions en solution de facilité, décidée à la va-vite, avec tous les risques d'abus d'un système mal ordonné.

Conclusion

Le rapport présente des propositions réalistes (c'est-à-dire dans le prolongement de ce qui est déjà entrepris et en fonction des techniques disponibles, sans tenter de réinventer le système de A à Z).

Elles portent entre autres sur :

- l'installation de lignes numériques permanentes sécurisées pour la réception par les enquêteurs des données utiles
- sur le regroupement à l'échelon interrégional et la mutualisation de ces centres d'interceptions
- sur la rationalisation des tarifs et des procédures des interceptions
- sur le contrôle autant en termes de bonne gestion que de libertés publiques,
- sur le matériel et les procédures,
- et sur une éventuelle extension des compétences de la toute nouvelle Délégation aux Interceptions Judiciaires. Sans empiéter sur le pouvoir du juge, cette innovation permettrait d'anticiper et de mieux vérifier le bon fonctionnement des interceptions judicaires.

Ouverture de la table ronde par le sénateur Jean-Jacques Hyest,
Président de la Commission des Lois

Le président Hyest rappelle comment le législateur est intervenu à la suite de scandales dans un domaine particulièrement sensible et qui touche aux libertés publiques : celui des interceptions. Le système des interceptions administratives dites de sécurité longtemps si contestées a fait l'objet d'une réforme profonde visant à en assurer le contrôle

Quant aux interceptions judiciaires, elles se sont multipliées dans le cadre de la lutte contre la grande criminalité, puis, plus récemment, contre le terrorisme. Seconde grande évolution : le changement des moyens de télécommunication, avec le risque que la législation conçue à un certain stade de la technique se trouve désuète ou inefficace à terme.

L'application de la Lolf, et les habitudes de meilleure gestion qu'elle a entraînées ont mis l'accent sur l'augmentation des frais de justice. Comme pour les fichiers d'empreintes génétiques, autre source importante de dépense, il est indispensable de rationaliser et de mieux contrôler la gestion des frais.

Après avoir souligné l'importance de solution conciliant efficacité et économie, le président rappelle un point effleuré par le rapport : la conservation des données issues des interceptions.

Intervention de Dominique Lotti, Chef de service adjoint du secrétaire général au Ministère de la Justice

C'est avec beaucoup d'intérêt que j'ai pris connaissance du rapport de l'Institut de criminologie de Paris qui, sur l'essentiel, et en tous les cas sur les constats, rejoint les conclusions du rapport Hirel auquel j'ai participé lorsque j'étais encore membre de l'IGSJ et les conclusions que je peux aujourd'hui tirer en tant qu'adjointe du secrétaire général et responsable depuis 1 an de la mission frais de justice rattaché au secrétariat général du ministère de la justice.

Vous le savez, la question des interceptions des communications est en effet depuis plusieurs années au cœur des préoccupations du ministère de la justice, en raison d'une part de l'importance que revêt ce moyen d'investigation dans la recherche de la vérité et la lutte contre toutes les formes de criminalité y compris bien sûr dans les affaires de terrorisme, d'autre part de leur coût qui ne cessait d'augmenter dans des proportions, on peut le dire vertigineuse, pour atteindre en 2005, 92 Millions d'euros presque 20% de la totalité des frais de justice. (sur un total de 487 M€)

Mais avant de parler chiffre je souhaiterai apporter quelques précisions sur les modalités de mise en oeuvre des interceptions judiciaires.

Il est, en effet, essentiel de rappeler qu'une interception judiciaire de voix ne peut être pratiquée que sur autorisation expresse d'un juge du siège, juge d'instruction ou juge des libertés et de la détention ; comme tout magistrat du siège, ils sont garants des libertés individuelles. Cette solution me paraît devoir être maintenue, notamment pour ce qui est de la compétence du JI en raison d'une part du fait qu'il connaît mieux que quiconque son dossier mais surtout de la nécessaire réactivité dans bien des affaires qui impose que la décision de placement sous écoute soit prise quasiment en temps réel.

Et contrairement à bien des idées reçues les juges sont soucieux du respect de la liberté individuelle et restent mesurés dans le nombre de placement sous écoutes et leur durée. Ainsi, le nombre des interceptions de voix est en France de 20 000 par an environ, ce qui est très inférieur à ceux d'autres pays : c'est 15 fois moins qu'en Italie, 12 fois moins qu'au Pays Bas, 3 fois moins qu'en Allemagne et quasiment équivalent à l'Angleterre, l'Ecosse ou l'Autriche.

Il faut, en outre, ajouter, que sur la masse des réquisitions judiciaires, la part des interceptions de voix reste limitée : en terme financier le rapport est de 30% à 70% pour les demandes de données de connexes (demandes annexes).

Enfin, sur la durée des interceptions, nous avons pu établir qu'elle ne dépassait pas, en moyenne, deux mois.

Par ailleurs, dans la détermination du choix du système à mettre en place pour assurer les interceptions judiciaires (écoutes et fournitures des données de connexion), il nous est vite apparu que ce système devait répondre à 3 exigences :

- mettre en place un dispositif techniquement efficace et évolutif qui puisse s'adapter en temps réel aux nouvelles technologies ;
- mettre en place un dispositif parfaitement sécurisé à un double titre : sécurité pour l'acheminement des données, sécurité pour assurer le respect absolu du secret de l'instruction ;
- enfin, mettre en place un dispositif performant au meilleur coût.

Après plusieurs études comparatives des différents systèmes possibles, il est apparu que le système centralisé était celui permettant le mieux de répondre à ces trois exigences.

En quelques mots rapides pour les raisons suivantes :

- Techniquement : parce que la création d'une structure centralisée, la DIJ, telle que cela avait été préconisé par le rapport Hirel, permet de disposer d'une veille technologique réalisée par des ingénieurs sous l'autorité d'un magistrat de l'ordre judiciaire et en coordination avec les structures interministérielles existantes ;

- Parce que la création d'une plate-forme centralisée sous le contrôle technique de la DIJ permettra des évolutions rapides de la centrale.

- l'assurance de la sécurité :que dire de ce point de vue du système actuel avec la multiplicité des sites et des matériels…. La centralisation permet sous le contrôle de la CNIL mais aussi d'une instance indépendante que nous envisageons de mettre en place pour assurer des contrôles réguliers d'assurer la sécurisation d'un système central et des liens pour les transmissions aux OPJ ;

Il convient d'ajouter qu'il n'y aura pas de conservation des données ;
Enfin, nous mettrons bien évidemment en place un centre de secours.

- Enfin, le coût : avec une plateforme national nous maîtrisons l'ensemble des coûts, sans risque qu'un jour on puisse nous opposer des révisions de tarifs que nous serions obligés d'accepter, dans la mesure où nous serions captifs, sans possibilité de mettre en place autrement les interceptions….

Quelques chiffres sur les coûts :

- la plateforme permettra d'économiser par an environ 45 M€ correspondant au coût de location des lignes de renvoi, au coût des fournitures de données par les opérateurs et bien sûr les coûts de location de matériel.
- Son coût de fonctionnement annuel est évalué à 7M€
- Quant a son coût d'investissement, il m'est difficile de donner ici un chiffre dans la mesure où la plateforme donnera lieu au lancement d'une procédure de marché.

Ce sont toutes ces raisons qui ont conduit le Premier Ministre, sur proposition du GDS a validé le projet de création d'une plateforme nationale. Les études vont débuter en 2007, son installation est prévue fin 2008, début 2009.

Il convient de préciser que dès le début de l'année 2007, nous disposerons d'une mini plate-forme pour l'interception des SMS et de certaines données.

Enfin un mot sur les tarifs des opérateurs de téléphonie :

- d'abord peut-être rétablir une vérité : il est vrai que les tarifs des opérateurs de téléphonie pour les prestations judiciaires étaient devenus trop élevés mais il faut expliquer pourquoi : d'abord parce que leurs prix unitaires avaient été fixés avant l'explosion de la téléphonie mobile, ensuite parce que si la justice payait à l'acte tel n'était pas le cas pour les interceptions administratives rémunérées au forfait, forfait non actualisé et il faut ajouter que certaines administrations de l'Etat on pu faire des demandes de fournitures de données de connexion sans les rémunérer….Il était donc important que ce dossier se traite au niveau interministériel, avec un arbitrage Premier Ministre et des tarifs uniques pour toutes les administrations. Donc sur les tarifs, tout n'est pas imputable aux opérateurs ;

- une révision des tarifs faite sur la base de la juste rémunération, principe constitutionnel. On pourrait imaginer, comme dans d'autres pays européens qu'il s'agisse là d'une obligation mise à la charge des opérateurs…

- des tarifs qui devront évoluer et sortir de la logique d'un tarif à l'acte, préjudiciable à la justice comme aux opérateurs.

Je souhaiterais terminer mon propos en rappelant que dans la relation opérateurs/ Etat et particulièrement la justice, il ne s'agit pas de relations commerciales. Nous sommes dans le cadre de réquisitions judiciaires auxquelles les opérateurs ont l'obligation de répondre, comme ils ont l'obligation de mettre en œuvre les moyens d'interception appropriés à tous les systèmes de communication. Ces obligations sont des obligations légales rappelées dans les textes.

Quand je parle d'opérateurs, j'entends non seulement les opérateurs de téléphonie mais également sur les fournisseurs d'accès Internet qui est aujourd'hui le secteur technique dans lequel nous travaillons également.

Intervention d'Alain Bauer, criminologue
ancien conseiller du Premier Ministre (Michel Rocard)

Le rôle du criminologue n'est ni d'interpeller les criminels ni de les juger, mais de comprendre leur mode de fonctionnement et les évolutions des phénomènes criminels, y compris dans l'usage des nouvelles technologies.

Le rapport présenté par François Bernard Huyghe et son équipe font, pour la première fois, le point sur un phénomène dont le développement avait été anticipé dans les années 90 par le Premier Ministre Michel ROCARD, lorsqu'il avait décidé de réglementer les interceptions administratives et de créer la CNCIS, outil moderne et efficace.

Le moment est donc venu de procéder à la même démarche pour les interceptions judiciaires et il faut saluer le travail considérable résumé dans le rapport HIREL et dans la contribution très précise et détaillée de Madame LOTTIN, représentant le Ministère de la Justice.

Il faut toutefois se méfier de pulsions nationales irrésistibles qui produisent toujours les mêmes effets : la tentation de l'Usine à Gaz, élaborée par des ingénieurs très compétents mais qui ne prendrait pas en compte toutes les réalités du terrain et toutes les problématiques de l'exploitation au quotidien.
Il faut aussi se méfier de la tentation de la Ligne Maginot électronique, qui écouterait tout et tous, au nom de la sécurité nationale, sans aucune capacité d'analyse. Trop d'écoutes tue les écoutes. Nos amis américains en ont fait la triste expérience en 2001 et depuis.

La chance du renseignement et de la police judiciaire en France (sous tous ses aspects, Offices Centraux, SRPJ, PJ de la Sécurité Publique, SR de Gendarmerie, etc.) est la qualité de son renseignement humain maintenu malgré les mirages technologiques.

Les mafias, le crime organisé et les organisations terroristes se servent sans difficultés du *High Tech* et du *Low Tech*. Il faut donc s'adapter à la réalité et ne pas rêver qu'elle s'adapte à l'organisation administrative.

Si la création de la Délégation aux Interceptions Judiciaires, dont la réalité interministérielle et la qualité des travaux doivent être soulignés, constitue un considérable progrès, la prise en compte des problèmes de maintenance et d'évolutions des technologies, qui bougent au quotidien, ne saurait être sous estimée.

Les précédentes initiatives, informatisation des commissariats ou des services du Ministère de la justice, plan calcul, etc.... n'ont pas laissé que de bons souvenirs lorsque le secteur public décide de traiter d'un sujet selon des principes de monopole sans véritable visibilité budgétaire....

Le maintien d'entreprises capables d'investir dans la Recherche et le Développement, capables de remplacer des équipements obsolètes ou dégradés dans des délais brefs, capables de garantir la proximité avec les équipes d'analyse, doivent faire l'objet d'une prise en considération, peut être sous la forme d'un Marché de performance plutôt que de simple équipement initial, comme le propose le Président Hyest. Si le sujet ne concerne pas les

interceptions de sécurité aujourd'hui, la gestion de cette plateforme nationale inspire déjà quelques préoccupations qu'on ne saurait mésestimer….

Sur ce sujet, comme pour le développement des empreintes génétiques, le nécessaire contrôle absolu du contenu des interceptions, élargi à tout ce qui échappe encore aux services régaliens (Sms, Skype, cartes prépayées, etc.....) nécessite de la flexibilité et une logique d'économie mixte pour éviter, dans 10 ou 15 ans, de se lamenter sur la paupérisation des systèmes, leur obsolescence, l'incapacité à s'adapter aux évolutions. Et de permettre une réduction substantielle des coûts.

A cet égard, la mobilisation des parlementaires pour imposer une obligation claire de service public à tous les opérateurs, devrait résoudre l'oubli dramatique de ces obligations dans le processus de privatisation et de dérégulation du secteur. Il faudrait même ajouter l'obligation pour ces mêmes opérateurs (téléphonie et Internet) de rendre aux policiers et aux magistrats les mêmes services (incluant la géolocalisation) que ceux proposés à leurs clients....

La mise en place d'un organe indépendant de contrôle des outils, dans le strict respect de l'indépendance des magistrats instructeurs, constituera également une avancée très positive. Et en attendant, la déclassification et la diffusion du rapport Hirel pourraient utilement servir à la compréhension des enjeux.

Intervention de Patrick Mauduit consultant, Synergie officiers

Nul aujourd'hui, ne peut nier l'importance extrême qu'ont prises, dans l'enquête policière « les interceptions de correspondances émises par voie de télécommunications » puisque telle est l'appellation judiciaire, selon les articles 100 et suivants du code de procédure pénale.
Importance extrême due à deux faits :

* le développement des moyens de communication ;

* les nouveaux outils juridiques fournis aux enquêteurs.

Les nouveaux outils juridiques

Depuis le mars 2004, est entrée en application la loi portant « adaptation de la justice aux évolutions de la criminalité », appelée Perben 2. Les nouveaux textes (article 706 – 93 du CPP) étendent les écoutes téléphoniques à l'enquête préliminaire, après accord du JLD, pour une durée de 15 jours renouvelables. Jusqu'alors, ces techniques n 'étaient possibles que dans le cadre de la flagrance (enquête de flagrant délit) et sur commission rogatoire (ouverture d'une information).

Le développement des moyens de communication

Développement qui non seulement est un tracas pour les enquêteurs par la multiplication des écoutes, comme du travail général vis-à-vis de la téléphonie, mais également avec une conséquence financière non négligeable.
Un exemple afin de donner une idée de ce que représente le développement de la téléphonie par rapport à l'enquête judiciaire :
* en 2000, le budget de la DRPJ de Paris était de 100 000 (cent mille) francs ;
* en 2006, les dépenses dans ce domaine dépassent les 500 000 (cinq cent mille) euros.
Développements exponentiels et, pour nous enquêteurs, effrayants.
Effrayant car le quotidien nous révèle chaque jour le fossé immense qui se creuse entre les techniques nouvelles, exploitées par les voyous de tous acabits et de toutes spécialités et les rares possibilités qui nous sont données d'exploiter les failles du système.

En prenant le risque d'inviter Synergie-officiers à cette table ronde, vous vous attendez certainement à ce que nous y jouions les trublions. J'ai lu le rapport rédigé par le département de recherches sur les menaces criminelles contemporaines et l'institut de criminologie de Paris avec beaucoup d'attention.

Il souligne la complexité des systèmes, les liaisons dangereuses entre la multiplication des téléphones portables et la grande délinquance, les problèmes techniques liés au développement du haut débit et du très haut débit qui permettent le dégroupage mettant à la disposition de tout particulier la possibilité d'utiliser la totalité du catalogue des communications…
Je cite un extrait de la page 36, qui m'a laissé un moment abasourdi : « Tout ce qui précède ne doit pas suggérer de généralisations excessives : la plupart des procédés pour prévenir les interceptions demandent du temps, de l'information ou de la formation, de l'intelligence, des moyens ou des efforts. Sauf peut-être la multiplication des cartes SIM, un principe très simple, tout cela n'est pas forcément à la portée du voyou ordinaire… »

Faux ! La réalité des services d'investigations est toute autre.
Ma démonstration n'est pas un cri d'alarme, mais un HURLEMENT D'EFFROI !
Ce rapport ne révèle que le sommet de l'iceberg.
Je vais vous parler de toute la partie immergée.

Les problèmes techniques de la téléphonie

Le rapport souligne parfaitement les deux inconvénients majeurs auxquels le policier se heurte :
* la piètre anticipation des changements technologiques… la mauvaise anticipation de l'explosion de la téléphonie mobile, responsable du volume des interceptions ;
* aucune négociation entre l'Etat, l'ARCEP – Autorité de Régularisation des Communications Electroniques et des Postes, le Ministère des Finances et les opérateurs au moment de l'attribution des autorisations, dans le domaine des obligations légales.

Les obligations légales

Ce sont les parcours obligés des quatre grands opérateurs français (France télécom, Orange, SFR et Bouygues) qui doivent, sur réquisitions judiciaires, permettre l'accès des enquêteurs à l'ensemble de leurs données, comme de leur permettre l'écoute de leurs clients, etc…

Ces obligations légales obligent également les sociétés de sous-traitance, chargées de gérer un certain nombre de lignes. Visiblement, elles ignorent la loi. Ainsi SFR sous-traite ses lignes à Coriolis, Universal phone, etc… Les réquisitions qui leur sont adressées ne servent à rien. Lorsque les réponses parviennent aux services enquêteurs, il est souvent trop tard. Reste aux policiers la vieille technique du terrain (surveillances et filatures) pour loger, puis identifier les contacts de leur objectif.

Le problème des MVNO (*Mobile Virtual Network Operators)* n'est toujours pas abordé : NRJ mobile, Breiz mobile, Virgin… (MVNO – opérateurs virtuels aqyant contracté des accords avec les opérateurs mobiles traditionnels pour acheter un forfait d'utilisation proposé à des clients)

Les erreurs de calage des balises

La totalité des communications par mobiles passe par les quatre grands opérateurs.
La presse a largement divulgué – lors de l'assassinat du Préfet Erignac - ce travail policier fait à partir des balises.
Les auteurs d'une infraction commise à une adresse précise se sont servis de mobiles. Des réquisitions sont adressées aux opérateurs. Quels numéros de balises ont été utilisés, durant

une tranche horaire précise ou plus large ? Les recherches obtenues, afin de vérifier l'exactitude des réponses, retour au terrain.

Quelques membres du groupe se transportent sur place, munis de leur portable personnel et de celui du groupe… Appels, puis nouvelles réquisitions adressées aux trois opérateurs. Souvent, de nouvelles balises apparaissent. Ce qui entraîne de nouvelles réquisitions par numéros de balise, afin d'obtenir les adresses et les numéros de cellules…

Le roaming / les appels en direction et en provenance de l'étranger à partir de portables
La technique actuelle permet de tracer un appel par mobile français, en provenance de l'étranger. Une réquisition judiciaire à Orange qui va interroger sa plate-forme internationale, afin de connaître l'opérateur utilisé. S'il s'agit d'un mobile vendu en France et utilisant un opérateur français, nous obtenons tous renseignements utiles, en échange d'un grand nombre de réquisitions judiciaires.
En revanche, nous nous heurtons à une impossibilité légale de tracer un mobile français fonctionnant sur un réseau étranger… Contrairement à un traité européen ratifié par la France, parce que le décret d'exécution n'est toujours pas publié. Le coupable (car j'ai le nom) est le secrétariat général du gouvernement qui n'a pas fait son travail.
Bien évidemment, il y a une impossibilité légale, sauf dans le cadre d'une CRI d'écouter un mobile étranger à l'étranger.

Les dérives de la téléphonie

Depuis l'ouverture à la concurrence du marché de la téléphonie, nous avons découvert l'existence d'une foule de petits opérateurs… Leur multiplication, comme leur disparition soudaine. (Plus de 100 opérateurs alternatifs ont obtenu l'autorisation de l'Arcep – autorité de régulation des communications électroniques et des postes)
Nombre de ces petits intermédiaires sont, parfois, inconnus de nos grands opérateurs et incapables de répondre à nos réquisitions.
Nous avons également constaté, au travers d'enquête les plus diverses que des particuliers se livrent à ce type de commerce en détournant à leur profit des contrats à forfait illimité, obtenus il y a 5 ou 8 ans, à l'âge d'or de la téléphonie… ou en se réabonnant ou se désabonnant auprès de nombreux opérateurs alternatifs…

Les numéros « hérisson » ou « passerelles »
Pour la majorité de ces petits opérateurs travaillant sous couvert de sociétés (notamment les taxiphones) leur logique économique est liée à l'impératif d'avoir des contrats avec un maximum d'opérateurs, le plus souvent étrangers. Ils peuvent ainsi jouer sur la concurrence et sur les facturations différentes d'un pays à l'autre. Lors d'une communication, en fonction de son horodatage et du destinataire de l'appel, le système choisit automatiquement le contrat le moins onéreux, afin de dégager la plus grande marge de bénéfice pour l'intermédiaire.
Cette opération, communément appelée « numéro hérisson » ou « numéro passerelle », se traduit par une renumérotation du numéro de l'appelant que l'on ne peut plus, ou très difficilement, identifier.

Les SMS
Nous nous heurtons à l'impossibilité légale de copier les messages textes adressés par mobiles.
Qu'en est-il de l'interception des SMS en judiciaire ?

Ce problème aurait pu être résolu en octobre 2005, grâce à un système de renvoi automatique des SMS par les opérateurs mobiles vers les boîtes E-mail des officiers de police judiciaire. La justice a fait blocage en décidant de ne pas choisir cette solution. Elle a préféré le faire elle-même en créant une plate-forme centrale… qui n'a toujours pas vu le jour et que nous attendons depuis deux ans.

Les cabines publiques

Les voyous continuent de se servir des cabines téléphoniques en toute connaissance de cause : il n'y aucune possibilité d'identifier la carte de téléphone utilisée, dès lors qu'il ne s'agit pas d'une carte France Télécom avec abonnement ou d'une carte bancaire.

Personne à ce jour, malgré de fréquents rapports dénonçant cette absurdité, ne s'est penché sur ce manque. Or la possibilité technique existe, puisque la société Tiscali / intercall est en mesure de tracer les cartes anonymes

Le problème des puces prépayées

Dans le cadre de toutes les enquêtes, nous nous heurtons au casse-tête que pose l'identification de l'usager d'un mobile fonctionnant par puces prépayées (Mobicartes, SFR La Carte, Nomad, ...) Le plus petit dealer, le plus minable des voyous utilise ce moyen de communications obtenu sous une fausse identité. Par connivence ou par facilité, les vendeurs ne vérifient pas l'identité de l'acheteur.

Trop souvent, aucune identité n'est relevée. Trop souvent, les voyous achètent des lots de puces prépayées, qu'il utilisent indifféremment ou selon un code d'emploi préétabli.

Il n'existe pas d'obligation légale de vérifier l'identité de l'acheteur, ni de peine associée à cette absence de vérification. Que fait le Parlement ?

L'usage des puces dissociées de leur boîtier

Tout téléphone mobile est composé d'un boîtier référencé par un numéro IMEI qui lui est propre et d'une puce dotée d'un numéro IMSI.

(IMEI – n° de série de l'appareil - Identifie de façon unique le téléphone / IMSI – attaché à la carte SIM – n° unique d'identification international d'un abonné mobile)

Nous rencontrons le même casse-tête lorsqu'il est fait un usage systématique de puces retirées des « packs prépayés» (puce et boîtier) vendus par les opérateurs. Cette dissociation entre la puce et le boîtier est, en soi, une fraude envers les opérateurs. Elle favorise l'anonymat des utilisateurs futurs desdites puces. De même, ces puces et ces boîtiers peuvent être « débloqués». Ces manipulations sont le fait de vendeurs ou de petits opérateurs peu scrupuleux et leurs clients les plus friands de ces puces, dont on a brisé le cellophane originel, des délinquants.

Altération du numéro du boîtier

Les nouveaux problèmes liés au dégroupage

L'arrivée récente sur le marché des communications du haut débit et du très haut débit permettant de recevoir chez soi, sur la même liaison téléphonique, la télévision, le téléphone et Internet à l'aide d'un boîtier fourni par chaque opérateur et appelé communément « BOX ».

(BOX – modem intelligent qui reconnaît TV, téléphone et net)

Si techniquement les interceptions sont possibles avec les opérateurs français, il n'en est pas de même avec les opérateurs étrangers… qui développent également des mobiles qui échappent à nos recherches.

Excellente transition pour aborder les difficultés rencontrés sur la « toile ».

Les problèmes liés au Net

La rotation des adresses IP des cybercafés
Bien que datant d'une dizaine d'années, l'activité économique des cybercafés n'est soumise à aucune déclaration spécifique. N'étant pas recensée comme telle, nous avons constaté avec effarement, l'impossibilité de lister les cybercafés, au cours d'une affaire récente d'enlèvement et de séquestration de personne..
Il est également impossible de constituer un annuaire fixe de ces cybercafés.

Nous devons alors systématiquement solliciter les FAI - fournisseurs d'accès Internet par des réquisitions judiciaires incessantes, afin qu'ils nous identifient l'adresse du cybercafé d'où a été envoyée la dernière exigence des voyous. Si le message transite par une hot line située à l'étranger…

De plus, ces cybercafés font également office de points-phones ou taxiphones. Etant bien entendu, qu'ils utilisent également la technique des numéros « hérisson » ou « passerelles ».

Les bornes Internet et les connexion sans fil

Oubli des obligations légales

Les opérateurs se soucient fort peu des notions de service public et d'intérêt général. En fait, ils connaissent ces obligations légales, mais elles ne les intéressent pas, puisqu'elles ne sont pas des sources de profits financiers.
Cette négation se répercute sur les personnels… négation à laquelle, il faut ajouter un certain mépris général de la police :
* de la part des opérateurs, nous constatons un manque de réactivité et de disponibilité les week-ends et les jours fériés de la part des personnels censés monter une permanence afin de répondre aux sollicitations de toutes sortes.
(ex : un week-end, il n'a pas été possible de mettre la main sur le permanencier Orange - Wanadoo, pour obtenir l'identification IP d'un cybercafé / alors que Wanadoo – Orange est le premier FAI en France)
* cette désinvolture des dirigeants entraîne un manque d'implication, de diligence et de sens des responsabilités de certains agents, en particulier au niveau des directions juridiques.
(ex : un soir, de semaine, la brigade criminelle a vainement insisté auprès d'une opératrice Orange-Wanadoo, soulignant que la vie d'une personne était en jeu, d'obtenir une identification. La personne a raccroché, puis fait parvenir la réponse un quart d'heure, plus tard, par télécopie… trop tard !)
Qu'en est-il du respect des dispositions légales du décret n° 93 – 119 du 28 janvier 1993 qui impose la présence d'experts qualifiés depuis au moins 2 ans dans l'entreprise pour répondre aux réquisitions judiciaires ? Les services d'obligation légale des opérateurs sont remplis à plus de 50 % de l'effectif par des personnels intérimaires ou en CDD récent. De plus, ces personnels ne répondent pas aux critères déontologiques prévus par le décret : à savoir leur habilitation par le procureur de la république du tribunal de grande instance, territorialement compétent.
Alors que nous avons constaté de nombreuses fuites, les opérateurs n'ont toujours pas procédé aux démarches administratives nécessaires !

Conclusions

A ce jour, selon les experts – ingénieurs informatiques ou des télécommunications qui travaillent avec nous - il n'existe aucune parade technique afin de lutter contre toutes les utilisations frauduleuses de ces nouvelles communications.
Par pur profit, les « inventeurs » continuent d'inonder le monde entier de ces innovations, ne se posant aucune question sur le mode d'utilisation de leurs produits. Avant leur mise sur le marché, ils ne soumettent jamais leurs innovations et les moyens de les intercepter aux forces légales.
Si ce rapport pose la généralité des problèmes concernant les nouveaux enjeux technologiques face aux évolutions de la criminalité et du terrorisme, il effleure à peine nos difficultés… et notre rancœur !
Les innovations techniques en matière de téléphonie et d'Internet ont mis entre les mains des malfaiteurs des armes par destination (les téléphones portables ont servi aux attentats de Madrid – gare d'Ochoa, et de Londres).
Par concurrence et appât du gain, les marques diffusant ces produits continuent d'ignorer leur extrême dangerosité, dès lors qu'ils sont détournés de leur usage normal. Pourtant, chaque jour, ils continuent de dépenser des fortunes en publicité pour vanter leurs produits, plutôt que d'en consacrer une partie pour la protection physique de leur clientèle… et aux interceptions !

Si demain, notre pays doit subir des attentats terroristes de la part d'individus utilisant toutes les lacunes techniques que je viens d'énumérer, nous policiers, ne pourrons pas les en empêcher. Nous aurons également énormément de difficultés à en identifier les auteurs. Lorsque des individus sont capables de détourner des avions de ligne pour s'en servir comme missiles, tout est à craindre… et je n'aborde pas le domaine de la cybercriminalité !
Personne n'aura le droit de se moquer de notre manque de réaction en la matière : malgré de nombreux rapports soulignant cette immense problématique, rien n'est fait et nous sommes toujours dans l'incapacité – technique et légale - d'apporter une réaction policière en temps réel.

Ce « m'en-foutisme » commercial a déjà fait une victime en France … et je salue la mémoire d'Ilan Halimi, torturé à mort. Sans être un technicien, ni un cerveau de l'informatique, mais un véritable cerveau de barbare, le chef de ses assassins a bénéficié de quelques conseils techniques, mais surtout de la sécurité zéro des modes de communications actuels, pour échapper à notre dispositif, après chaque appel passé à la famille de sa victime !

Je sais que mon introduction – coup de gueule - est trop longue et pour cela je n'aborderai pas le volet enjeux budgétaires, que je considère comme du racket de la part des opérateurs, comme des fournisseurs d'accès… maintes fois dénoncé par Synergie-officiers…

Propositions

Dans le cadre d'événements majeurs (affaire d'enlèvement, terrorisme) :
* mise en place d'un centre opérationnel avec tous les opérateurs en téléphonie / Internet, et les services de police concernés. (Il est indispensable d'obtenir des informations techniques en temps réel permettant la localisation instantanée du lieu d'une connexion Internet des ravisseurs qui consulteraient la « boîte aux lettres » dédiée aux communications avec la famille.)
* que l'ensemble des opérateurs en téléphonie utilisent le même format pour les réponses (factures détaillées notamment), format qui rendrait plus aisé et plus rapide l'intégration et le croisement des données.
* un accès Internet sécurisé et contrôlé par un mot de passe spécifique et temporaire, réglé forfaitairement, à l'annuaire des opérateurs de téléphonie mobile.
* une disposition légale permettant d'alléger la procédure. (Une réquisition générale à l'opérateur avec ensuite une formulation plus souple - mail - pour chaque demande et non, comme aujourd'hui, une réquisition judiciaire à chaque sollicitation policière).

* La création - au même titre que le personnel technique et scientifique – d'un corps d'ingénieurs et d'agents des télécommunications, au sein de la police nationale. La complexité de la téléphonie et de l'Internet, dépasse aujourd'hui les compétences des enquêteurs.

Intervention de Michel Besnier, consultant, Elektron

Evolution des techniques et des coûts d'interception

Ces dernières années, les Interceptions judiciaires ont fonctionné, et fonctionnent encore pour une partie, sur un système archaïque à tous points de vue.

Ce qui a bloqué longtemps l'évolution des moyens d'interception, ce sont avant tout des difficultés juridico-administratives. En effet, le paiement à l'acte a engendré une mise à disposition à chaque fois d'une ligne France Télécom temporaire, par nature extrêmement coûteuse, permettant de renvoyer la voix du GSM.

Le système impliquait également la location d'une machine au coup par coup, obligeant les « loueurs de machine » à gérer la logistique correspondante. Par ailleurs, ils devaient concevoir et fabriquer des machines pour environ 3000 écoutes, en petites séries, ce qui générait des coûts très importants, lesquels étaient bien sûr répercutés à la Justice.

Elektron a lancé, en 2003, des plates-formes centralisées, qui généralement sont installées dans les principaux centres de Police et de Gendarmerie, et qui permettent l'acquisition numérique de 200, 300, 400 ou même 500 lignes, soit largement au-delà de ce qui est nécessaire pour les grands centres de Police et de Gendarmerie.

Les lignes de renvoi temporaires France Télécom ont pu alors être remplacées par une arrivée numérique installée en permanence, que la Justice ne pouvait pas prendre en charge sous cette forme. C'est pourquoi, avec l'appui de la commission Hirel, Elektron a obtenu l'autorisation d'installer le premier renvoi numérique à ses frais, connecté à une machine fournie par ses soins, permettant de donner à la Justice et à la Police bien sûr, un système globalisé, installé en permanence.

Outre la réduction de coût, cette opération a permis de faire des mises en œuvre extrêmement rapides des écoutes. La ligne de renvoi et les machines étant disponibles de manière permanente, une simple réquisition suffit à mettre en place l'écoute, en quelques minutes, alors que cela demandait auparavant plus de 24 heures.

Les machines aujourd'hui ne sont en fait que des serveurs, ordinateurs de marque connue, très fiables et peu coûteux. Ce sont les logiciels que nous avons développé qui représentent la réelle valeur de l'équipement. Au total, cette procédure a permis de baisser les coûts pour la Justice d'environ 60%.

Ce nouveau système a également permis de donner aux enquêteurs des moyens qu'ils n'avaient pas. Avec les anciennes machines, les enquêteurs avaient l'obligation de passer du

temps dans les salles d'écoute quand ils voulaient faire une écoute directe, puis de ramasser leurs disques et de revenir dans leurs bureaux, donc des allées et venues, des pertes de temps. Aujourd'hui, nous installons un câblage et des PC portables dans les bureaux des enquêteurs, et chacun peut de son bureau suivre son enquête, avoir des écoutes directes tout en travaillant sur autre chose, appeler de son mobile le serveur pour consulter les communications en cours, etc.

Pertinence d'un système mixte Etat/Privé

Il faut garder à l'esprit que les écoutes judiciaires doivent être exploitées par les enquêteurs sur le terrain. Prenons l'exemple d'un gendarme qui met sur écoute des cibles en Auvergne pour un enlèvement. Il est bien évident que ce n'est pas un grand service parisien qui va devoir écouter les personnes surveillées, mais bien l'enquêteur dans son village, parce que c'est lui qui a besoin de suivre son enquête. Une distribution instantanée des données aux enquêteurs est donc nécessaire.

Ainsi notre métier n'est pas celui de l'Etat. En effet, nous sommes toujours là pour mettre à disposition efficacement les moyens nécessaires à l'enquêteur. Nous remplaçons immédiatement un PC en panne, assurons une formation permanente, offrons au fur et à mesure des fonctionnalités supplémentaires. Des problèmes administratifs ou juridiques, comme des limitations budgétaires, notamment, n'entrent pas en ligne de compte, notre priorité étant de fournir aux enquêteurs le meilleur service possible.

Surtout, il faut considérer les efforts fournis depuis 3 ans, spontanément, par Elektron, pour mettre en place des systèmes plus modernes et plus économiques. Ce ne doit donc pas être un problème pour l'Etat que de sous-traiter à des privés, qui, mis en compétition, doivent toujours être toujours au maximum de leurs possibilités pour suivre les techniques nouvelles, et pour offrir des tarifs compétitifs.

Considérons également les obstacles juridiques et administratifs auxquels se heurte souvent l'Etat, et devant lesquels les privés sont forcément plus souples et plus réactifs. Ainsi, il y a plus d'un an, nous avions proposé à la Justice de fournir immédiatement et sans supplément de prix, les SMS et les IRI. En effet, nous avions à l'époque pris des accords avec Alcatel, qui nous fournissait l'équipement correspondant.

La Justice craignait alors qu'Elektron obtienne un monopole de fait, et n'a pas donné de suite positive.

Ce genre de blocage ne préfigure-t-il pas ce que pourrait être un système d'Etat : les nombreux problèmes juridiques et philosophiques qui se poseraient pourraient entraver son bon fonctionnement, et même sa réalisation.

Cela prouve en tout cas que les sociétés privées sont capables d'amener les techniques, les évolutions, les prix. On sait tous que pour des sociétés comme les nôtres, c'est le seul moyen de subsister et de pérenniser notre activité.

Nos voisins européens font largement appel aux privés pour leurs interceptions téléphoniques, et les administrations françaises le font également pour les analyses en laboratoire nécessaire aux enquêtes, pour l'entretien des parcs automobiles, et pour d'autres types de services.

Conclusion

L'établissement de plates-formes gérées par les privés sous contrôle de l'Etat, même si l'acquisition centralisée (interface avec les opérateurs) passe par une plate-forme nationale, est la meilleure solution pour l'exploitation des interceptions judiciaires incluant la voix, les SMS, les IRI, et toutes les nouvelles techniques de communication."

Annexes

AVANT

Réquisition

Trois intervenants : France Télécom active la ligne de renvoi, puis l'opérateur GSM et le loueur de matériel et de services interviennent.

Mise en route

Délai pour la ligne France Télécom : 24 heures
Puis renvoi de la ligne GSM
Ensuite livraison de la monovoie.

Fonctionnalités

Acquisition voix seulement, qualité analogique.

Une salle d'écoutes est nécessaire dans chaque Centre avec installation de plots (en nombre limité) pour l'acquisition et le gravage des CDs.

Va et vient des OPJ de la salle d'écoutes vers les PCs d'exploitation installés dans leur bureau.
Ecoute directe : nécessite de rester des heures dans la salle d'écoutes.

Coût

Paiement à chaque fois de l'activation de la ligne de renvoi France Télécom.
Cherté des monovoies : fabrication en petites séries et logistique entrée/sortie.

Coût des fadets GSM (mails des opérateurs avec les Informations Relatives aux Interceptions) du fait de l'impossibilité pour les monovoies de les recevoir.

Sécurité

Pas de contrôle centralisé des ouvertures / fermetures de lignes.

Difficulté de contrôle des effacements de disques durs des monovoies aux entrées/sorties.

APRES

Réquisition

Deux intervenants : l'opérateur GSM et le fournisseur de services, qui intègre les lignes de renvoi permanentes numérisées France Télécom, et l'activation du matériel nécessaire à l'acquisition / exploitation des écoutes (lequel est en permanence dans les Centres d'Ecoutes).

Mise en route

Immédiate

Fonctionnalités

Acquisition numérique de la voix, des SMS, des IRI et d'Internet sont possibles.

Un serveur plus un réseau dédié desservent les bureaux des OPJ du Centre principal et des Centres distants.

L'OPJ travaille totalement depuis son bureau y compris pour l'écoute directe.
Il peut accéder à distance au serveur de manière sécurisée depuis un fixe ou un mobile, ou se faire renvoyer les appels sur son fixe ou son mobile.

Coût

La mutualisation des systèmes comprenant les lignes de renvoi permanentes permet de diminuer les coûts de ces postes de plus de 60%.

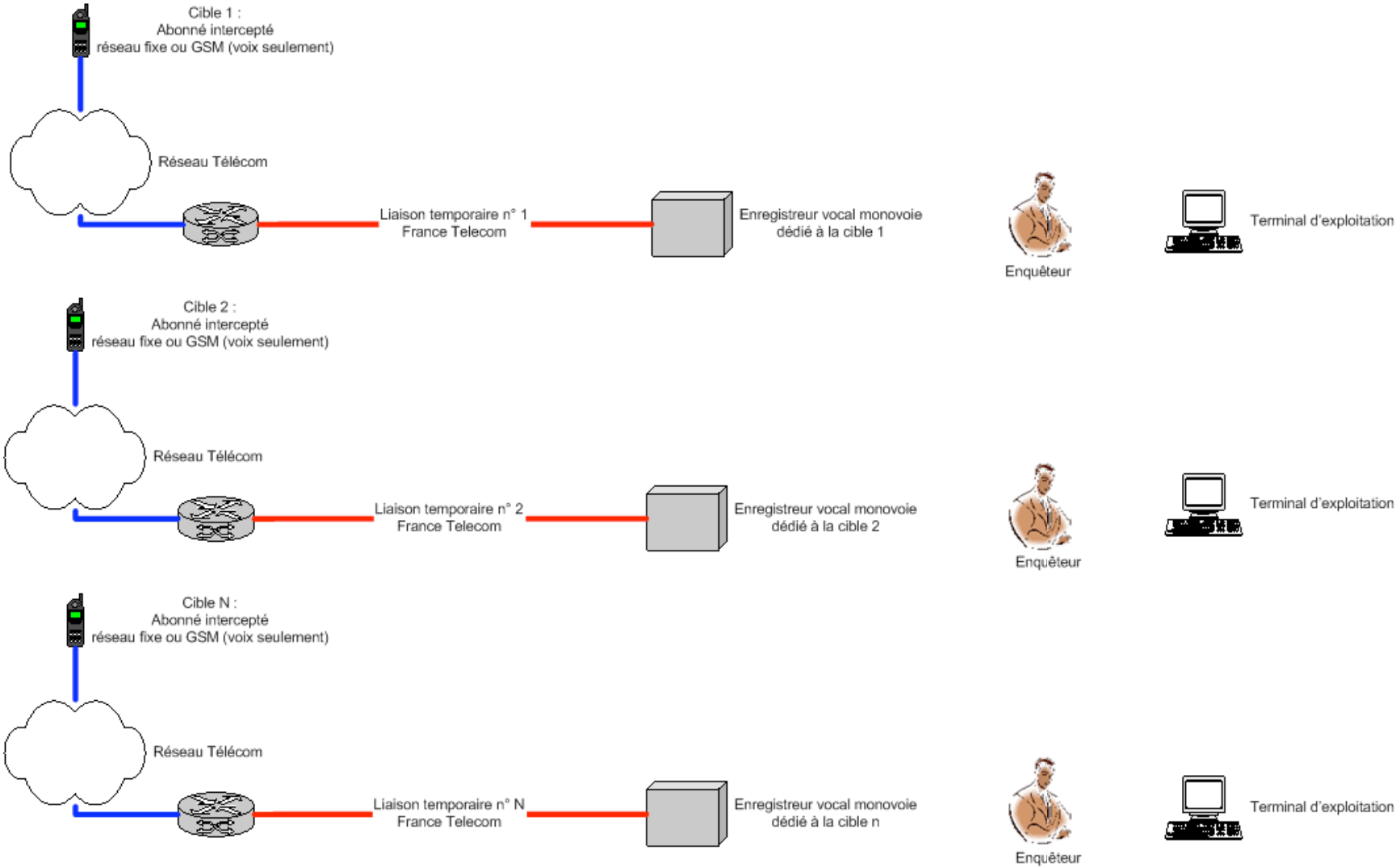
L'acquisition automatique des SMS / IRI permet de réduire considérablement ce poste.

Sécurité

Un administrateur désigné peut suivre les ouvertures / fermetures de lignes, gérer les statistiques.

Le matériel reste en permanence dans le Centre d'Ecoutes.
Les disques durs sont laissés au Centre lors de leur changement en fin de vie ou pour des raisons de maintenance.

Concept des interceptions analogique monovoie



Concept mutualisé des interceptions multilignes numériques