

## **Paranoïa : tous surveillés, tous fichés, tous fliqués**

10 Dec 2008

Tous surveillés, tous fichés, tous fliqués : une théorie du complot ?

Tous surveillés : les écoutes, les caméras, dans la rue, à la banque, dans les entrées d'immeubles.

Où l'on revient d'abord sur les Ecoutes. Les internautes sont si stupéfaits qu'on ose mettre en cause leur bébé, leur bijou, le réceptacle de tous leurs secrets qu'ils sont entrés en fureur, quand je leur ai expliqué que leur charmant petit téléphone portable est non seulement écouté en permanence - quand c'est nécessaire - mais encore qu'il sert à l'occasion de micro espion. Tout comme votre téléphone fixe, il faut bien le dire. Et plus le téléphone est sophistiqué, genre Iphone, Blackberry ou concurrents, plus les écoutes sont développées. A la suite de mon papier sur les Ecoutes, de nombreux, d'excellents ingénieurs, experts, spécialistes, sachant et tout ce qu'on veut, se sont répandus en invectives pour me taxer d'ignare, d'affabulateur, de fantaisiste. Naze. Journaliste débutant, qu'il aille ailleurs apprendre son métier. Ce serait une honte pour rue89 d'accueillir une telle contribution. J'en passe car je reviendrai sur cet étrange comportement linguistique dans un autre billet. Ils rigolent, ah, ah, Madelin est un imbécile intoxiqué par un faux informateur. Un maniaque du complot généralisé. Tonalité générale de la plupart : on n'y croit pas. Comme si des faits étaient une question de foi. On pense que c'est impossible, donc on n'y croit pas.

Malheureusement les remontées techniques vont toutes dans le même sens. Oui, on peut vous écouter en tous temps, en tous lieux, dans n'importe quelles conditions. Téléphone ou portable inactif. Non seulement on peut vous écouter, donc vous enregistrer, mais encore on peut vous localiser avec une précision qui reste à déterminer, entre cent mètres et quelques mètres, vous localiser et vous suivre à la trace (roaming). Et pas seulement en temps réel. Toutes les données enregistrées sont conservées en mémoire durant deux ans, et les fournisseurs sont tenus des les livrer aux Autorités de police et de justice à la première réquisition judiciaire.

Est-ce clair ?

Même topo pour votre messagerie internet, sécurisée (https) ou non (http), pour vos SMS. En bref pour tout ce qui cause, se transmet, par fil, par radio, par informatique. Pour l'ensemble de ce nouvel univers virtuel dans lequel nous baignons, dans lequel nous nous noyons.

Il apparaît en outre que des logiciels disponibles sur le Web permettent à des personnes non habilitées - sinon mal intentionnées - de mettre en place de tels systèmes d'écoute et d'interception. En revanche, je ne dispose pas d'éléments permettant de soutenir et d'affirmer que les appareils photo et les caméras intégrées dans certains portables puissent être utilisées à des fins de surveillance, hors contrôle du propriétaire. Alors, acheter un portable pour un usage unique, et ensuite le jeter ? En principe, ce n'est plus possible, ni en France, ni en Suisse, l'achat d'un portable à carte nécessite la production d'une pièce d'identité. Mesures de lutte anti-terroriste obligent.

Parlons de l'image maintenant. En principe, la législation sur la protection de la personne privée interdit de prendre des photos d'inconnus, sans leur consentement, sans leur autorisation, et encore n'est-ce pas toujours suffisant.

Ce n'est pas vraiment un problème pour les autorités de police, publiques et privées, qui prennent en charge notre sécurité. On frémit en imaginant les 10.000 caméras - ou plus - en service à Londres pour traquer... Les incidents de circulation... Les banlieusards qui entrent en ville sans avoir payé leur abonnement... les petits voyous... Les passagers du métro, dans les gares ou dans les aéroports. Ces Anglais, quand même, on les croyait démocrates. Eh bien, s'ils ne sont pas démocrates, nous non plus. Dans le sous-sol de la Préfecture de police à Paris, sur les écrans d'une salle de surveillance aboutissent des images filmées dans toute la capitale. Hier, quelques centaines de caméras, toutes fixées assez haut pour que de mauvais plaisants ne puissent les détruire. Des milliers de nouvelles caméras vont s'ajouter au système le plus ancien. Ce n'est pas tout : toutes les grandes stations du métro parisien, toutes les grandes gares, sont sous surveillance continue. Tout comme les bus, toutes les lignes sont équipées

progressivement. Et mieux encore : toutes les agences bancaires, et maintenant de nombreux magasins, petits ou grands, des supermarchés aux supérettes. Si je compte bien, on n'est déjà pas loin des 10.000. Et ce n'est qu'un début, tout le monde en veut. Et c'est d'autant plus facile que les caméras coûtent de moins en moins cher. Elles tournent en permanence. Le moindre site touristique vous propose un visionnage de la ville en continu.

Alors, rester chez soi, en coupant le téléphone ? Mais comment se distraire : reste la télévision. Là ce sont les outils d'audimat qui scrutent votre comportement ; c'est google qui vous traque. Et ce n'est pas vraiment nouveau. Le 8 juin 2006 il est révélé qu'une équipe de recherche Google a mis au point un prototype qui se sert du microphone interne de l'ordinateur personnel pour écouter dans une pièce, déterminer ce qui est regardé à la télévision et à offrir sur le Web des informations supplémentaires. En général, ce genre de prototype ne reste pas bien longtemps dans les tiroirs.

Et quand vous en aurez fini avec le son et l'image, restent les fichiers. On a beaucoup glosé sur les fichiers EDVIGE - devenu EVDISRP - , et CRISTINA en service à la DCRI. Dans un rapport remis aujourd'hui même 9 décembre, le criminologue Alain Bauer répertorie 44 grands fichiers de police. ADN, condamnations pénales, infractions routières, suspicion de terrorisme, tout y passe. En vérité, tant de fichiers sont en service qu'il est presque impossible de ne pas tomber dans leurs filets. Sans compter les fichiers des Impôts, des banques, des mauvais payeurs, des interdits bancaires.

Allons, n'en jetez plus. Nous ne sommes pas en plein complot, mais dans la réalité

## **Paranoïa 2 - A ceux qui lisent**

10 Dec 2008

Parmi les centaines de réactions enregistrées après mon papier dans rue89, une très grande majorité expriment des doutes, une "absence de foi", et m'invectivent avec allégresse, le plaisir de la dénonciation anonyme. J'en ai trouvé cependant quelques unes qui ciblent un peu mieux le problème. Un problème de société que je ne soupçonnais pas vraiment. Mais aussi un problème politique.

mimitos | infoman 14H19 08/12/2008

ben voyons, il est bien plus facile de contester que de penser, de dénigrer que de réfléchir, de laisser ses mains dans ses poches au lieu de faire des grands signes ! Au bas mot : 80% de la population est composée de moutons incapables de réfléchir par eux-mêmes, sans arrêt en train de copier sur l'autre, trop dur de s'émanciper...

Croyez qui vous voudrez, mais je trouve cet article intéressant et pas bidon.

Vous êtes vous posé la question simple : au dos de ma carte d'identité, qu'est ce que c'est que cette petite bulle dans mon adresse ?

Peu de gens se la posent et pourtant il y a des réponses...mais faut se poser la question...d'abord !!!!

merci pour cet article MR Madelin, et ne raccrochez pas, il y a ici des gens qui vous lisent et qui vous apprécient !

Kid\_A 00H07 09/12/2008

Au regard du grand nombre de réactions, ce sujet marque un point: il y a un véritable attrait pour ce genre de petites choses qui toucheraient à un « complot ». Pour recadrer les divers points, les confirmer, les infirmer, les démontrer... Les réactions sont variées.

J'avoue qu'après en avoir lu certaines, on y trouve le blanc et le noir. Je vais continuer à tourner en rond.

Mais je me demande quelles sont les connaissances du grand public en matière de haute technologie, la plus haute pointe. Le « top-secret » existe bel et bien non?

Alors qu'en est-il?

Le portable tente de devenir petit à petit l'élément indispensable à toute vie sociale, communications, médias, paiements divers... ou bien télécommande, vibro, réveil pourquoi pas...

Ils sont de véritables petits émetteurs de notre vie, et s'étendent toujours davantage. Et c'est sous contrôle certain, on ne peut le nier.

Un lecteur a écrit que ce genre d'article n'avait sa place que sur un site du genre conspirationniste. Ce que j'aimerais dire, c'est qu'à l'heure de la délation ouverte, des appels d'offres pour surveiller le net, traquer et dénoncer(et j'en passe), un nombre aussi important de réactions sur certains articles qui fleurissent sur ces sites « toutpabos », ne seraient pas un mal pour la réflexion que lancent ces mêmes articles. J'imagine que ça permet d'avancer.

Il n'y a pas de « théorie du complot ». Pourrait-on utiliser le mot « pratique »...

A moins qu'aucun homme de pouvoir, avide de conquête, n'existe sur cette terre.

Après tout nous serions une génération chanceuse, l'Histoire ne nous apprendrait plus rien, et rien ne nous menace, pas mal un téléphone portable.

Redroom 11H40 09/12/2008

Moi je suis désolé mais autant de réactions négatives sur un sujet aussi bateau, je trouve ça louche, vraiment vraiment louche.

Je crois surtout que les gens sont devenus complètement accros à leur téléphone portable et ils le défendent comme on défend son « bébé » c'est à dire en toute subjectivité.

Cet amour aveugle pour un simple objet de consommation courante est troublante et inquiétante...

piaf | visiteur 14H21 09/12/2008

Même si cet article n'est probablement pas le mieux écrit et le mieux documenté du genre, je m'interroge grandement sur les commentaires si péremptores de certains internautes. Beaucoup d'argument d'autorité (« Je suis professeur d'électronique », « je suis ingénieur en télécommunications », etc), mais peu d'arguments réels. Qui peut garantir qu'un appareil aussi complexe qu'un ordinateur (un téléphone n'est qu'un ordinateur doté d'un émetteur) fonctionne comme marqué sur la notice ?

Toutes ces personnes à l'avis si tranché sont-elles mandatées par nos chers services de renseignement pour faire de l'intox ?

Merak | pré retraité 22H28 09/12/2008

c'est du grand n'importe quoi ce grand n'importe quoi . étonnant tous ces gens qui savent bien. étonnant. y savent bien pour la conception des vlsi spécialisés dont le masque est protégé, du logiciel embarqué, libre forcément, des normes et standards à peine stabilisés. de la crypto dans ses moindres détails. Et de tant de choses encore. Et tous ingénieurs avec ça, dans les télécoms, bien sûr. Tous ces très braves gens se souviennent sûrement des fonds baptismaux du GSM, voire même de Rita. Quand même, qu'elle date que celle de Mais 68. Passionnant ce fil.

## **Paranoïa - Suite et fin du débat sur les écoutes**

11 Dec 2008

Je ne suis pas las du débat sur les Ecoutes, mais il tourne en rond en raison de l'acharnement de quelques correspondants. J'apporte une dernière réponse globale. Ensuite je passerai à autre chose.

En italique quelques propos basiques d'un des plus ardents blogueurs. En romain, mes réponses globales.

Je suis accusé de propager des rumeurs urbaines, pour terroriser les foules.

Il n'y a pas de rumeur, propagée par désir de sensationnalisme alarmiste, dans la perspective d'une fumeuse « théorie du complot » dont je serais une adepte, mais des faits recoupés par de nombreuses sources. D'ailleurs, vous vous gardez bien de relever les éléments fournis pas la suite en complément du travail sur les écoutes, enregistrements filmés et fichage. Je vous rassure, dans les quelques centaines de posts reçus, près de la moitié traitent de la question technique. Je vous répète que celle-ci était hors de mon propos.

Reprenez vous Mr Madelin, ça arrive à tout le monde de se planter, apprenez l'humilité, nous sommes tous encore prêts à vous écouter du moment que vous ne dites pas (encore) n'importe quoi.

A partir du moment où l'on pense qu'une personne est dans l'erreur et qu'on le lui signale, on a toujours tendance à lui "faire la morale"...pour ma part je pense que le travail d'information n'a pas été fait, ou alors mal fait...ne rien dire est de la complicité...le dire est moralisateur...j'ai fait mon choix.

Les blogueurs sont très sûrs d'eux, mais ils voient la paille dans l'œil de l'autre, pas la poutre dans le leur. Ils reprochent à mon texte l'absence de preuve, mais ils sont eux-mêmes incapables de soutenir la moindre argumentation cohérente. Ils n'apportent pas la moindre contre preuve aux éléments que je soutiens, que je résume, et, comme toujours, chaque mot a son importance, on ne peut pas tirer n'importe quoi d'un mot, pour arranger son opinion personnelle. Voici ce que j'ai écrit pour l'essentiel, dans une perspective strictement politique :

1 – Tous les portables peuvent être interceptés, dans n'importe quelles conditions, durant les périodes de communication.

2 – Cette possibilité d'interception, accompagnée de la géolocalisation à l'origine du roaming, se prolonge lorsque le portable est en veille, puis quand le portable est fermé, mais batterie active.

3 – Mon interlocuteur a évoqué la possibilité de localiser un portable dont on aurait retiré la batterie. Je présente ça comme une hypothèse, et non comme une certitude.

Vous voulez absolument une démonstration, des preuves, alors que ce billet n'a aucun vocation à être un document scientifique. Contrairement à certaines opinions tout à fait diffamatoires, je suis un journaliste fort sérieux, malheureusement trop sérieux, au demeurant. Si ça vous intéresse tellement de savoir comment je travaille, reportez-vous à mes livres, tous disponibles à l'achat sur Amazon.fr. En particulier le dernier « Dans le Secret des Services », chez Denoël.

Je vous rappelle que la législation sur l'injure et la diffamation, loi de 1881, s'applique aussi aux correspondances transmises par internet et publiées sur des blogs.

Je n'ai pas senti de "fureur" dans mon commentaire, un peu de mesure je vous prie.

Quand je parle de « fureur », je vise l'extrême vigueur de vos propos, de vos remises en cause morales, qui rejoignent les commentaires du même acabit. Et votre volonté de « me faire avouer ma faute ». Curieux langage religieux pour un sujet qui ne l'est pas.

le débat est plus intéressant du côté des "concertés" (oui, tout ces monstrueux anonymes qui se sont concertés pour dénoncer votre article, sur ordre des gouvernements du monde...).

Je n'ai rien suggéré de ça. Je constate seulement l'étrange conjonction des propos qui cherchent à démolir ma réputation. Des propos sans effet, je vous le précise : sur 78.000 visites, on a relevé seulement une centaine de posts critiques et véhéments. Je sais aussi compter : 0,0073333 %, c'est-à-dire moins de 1 pour 10.000. Et soyez rassurés : si les fournisseurs d'accès se sentaient affectés, s'ils avaient eux-mêmes des contre-arguments à présenter, ils me les auraient déjà transmis.

## **Ecoutes, polémique : les internautes informateurs**

07 Dec 2008

L'article sur les Ecoutes : avalanche de polémiques 2

Mon article sur les Ecoutes sophistiquées publié sur rue89 a donc provoqué une avalanche de réactions, et, de façon assez curieuse, de graves doutes quant à mes sources et à mes compétences techniques. De nombreux intervenants mettent en cause la qualité de l'information véhiculée par cet article, tout en apportant de bien intéressantes précisions. Je vous en rapporte l'essentiel, assorti de réponses.

Oui, on peut mettre quelqu'un sur écoute (quand on voit les démarches administratives quand on ouvre une ligne de téléphone mobile, c'est fait dans le sens que la carte SIM est associée à une personne physique). Mais ça n'est pas à la portée de tout le monde d'espionner parce que chaque conversation est cryptée et tous les cryptages ne sont pas tombés dans le domaine public,

Les interceptions de communication, se font toujours au niveau du filaire, dans les bon vieux centraux, et oui la voix passe par beaucoup d'infrastructure terrestres avant de passer d'un tel à l'autre.

Cet intervenant n'est pas très en avance. Il y a belle lurette que les bons vieux centraux ne sont plus utilisés pour les écoutes, il suffit d'une émission radio électrique pour que soit effectuée l'interception.

Il n'y a pas besoin de commission rogatoire pour que la police accède a ces données (donc zéro contrôle de l'autorité judiciaire), n'importe qui dans un commissariat peut envoyer un fax à Orange pour avoir ces infos.

Inexact. Aucun commissariat ne peut demander des écoutes directes. Comme je l'indique, c'est ou une commission rogatoire délivrée par un juge pour la PJ, ou une demande formelle au cabinet du Premier Ministre pour les écoutes administratives.

Les écoutes proprement dites sont censés être effectuées uniquement après autorisation d'un juge, mais vu le nombre de dossiers qu'ils voient passer les vérifications ne se font pas de façon approfondies.

Les opérateurs GSM conservent les données de connexion de tous les utilisateurs pendant deux ans. Ces données contiennent le numéro du correspondant, la durée de la communication mais aussi toutes les informations de roaming (le passage d'une cellule GSM à une autre).

Le plus inquiétant c'est les données de roaming, ça veut dire que si vous possédez un téléphone portable, et que vous le laissez allumé, on peut savoir tous les endroits où vous vous êtes rendu avec une précision de l'ordre de 50m à 200m (par triangulation).

On peut donc par exemple savoir que vous êtes souvent à proximité de tel ou tel personne,

« N'importe quel bon bidouilleur informatique peut intercepter votre téléphone » : mais oui, c'est cela, tout informaticien est méga omniscient omnipotent ... « Bon » doit désigner une catégorie que je qualifierais plutôt de « extrêmement pointue » actuellement ?

Peut-être ...

J'arrête là, on \*peut\* (surtout la NSA ?) faire beaucoup, intercepter beaucoup. Je serais responsable des réseaux au gouvernement, je préférerais acheter du matériel français ou européen plutôt qu'américain. Mais l'article n'apporte aucun élément factuel et tombe dans la paranoïa complète.

Pour le téléphone éteint encore allumé, ce n'est pas strictement impossible, mais à la base il s'agit d'une légende urbaine qui a subit le téléphone arabe.

Ecoute par un téléphone éteint, mais avec batterie en service, première réaction :

L'écoute téléphone éteint, c'est n'importe quoi sur les modèles courants et aujourd'hui (le futur, je sais pas le prévoir) tout simplement parce que lorsqu'on éteint le téléphone l'alimentation des circuits du modem GSM/EDGE/GPRS ou UMTS sont coupés. Sans eux, pas de communication possible entre votre portable et l'antenne BTS.

Ensuite, tous les intervenants admettent que c'est possible.

Pour ce qui est de l'écoute « ambiante », aucun procédé de ce type n'est prévu ni dans la norme GSM/GRPS/EDGE ni dans sa variante DCS ni dans la norme 3G/UMTS/HSDPA.

Pour que cela soit possible il faudrait que ces normes établies par le CEPT (European Conference of Postal and Telecommunications Administrations) soient volontairement falsifiées pour le grand public et que tous les acteurs du secteur soit dans le coup (une centaine de constructeur et plus de 300 opérateur dans le monde ainsi que toutes les sociétés sous-traitantes).

Je rappelle que les lois antiterroristes en vigueur aux Etats-Unis – Security Act - imposent à tous les constructeurs et à tous les opérateurs de communiquer leurs données techniques pour que les services d'écoute, notamment de la NSA, puissent intercepter toutes les formes de communications.

Personnellement je suis plus dubitatif quant à la géolocalisation d'un téléphone sans batterie, mais mon interlocuteur a été formel. Il est probable que ce n'est envisageable qu'avec des outils utilisés par les services de renseignement. Précision d'un internaute :

L'écoute téléphone éteint, pourquoi pas. Le micro, et même le haut parleur génèrent de l'électricité, et donc des ondes électromagnétiques, avec ou sans batterie, fils coupés ou non.

Pour ce qui est « d'allumer » le téléphone à distance, je suis là effectivement dubitatif, il faudrait pour ceci que le téléphone soit prévu pour, et 1/ cela se saurait

On évoque bien le cas du téléphone éteint, mais batterie en place, donc avec une source d'énergie.

2/ cela serait détectable relativement facilement (impossibilité de téléphoner pendant qu'on est écouté, bruit caractéristiques dans les enceintes qu'on connaît tous bien, et surtout batterie qui ne dure pas.

L'écoute fonctionne comme une téléconférence, elle n'est active que lors d'un appel.

Les services ne manifestent pas dans la rue pour rendre publiques leurs dernières trouvailles. On est ici dans la course entre la serrure et le cambrioleur, une course qui ne cesse jamais.

Il existe des 'exploits' permettant de prendre la main sur un système donné et ce que dit cet article est possible sous réserve de plusieurs éléments.

Certes les portables sont devenus de véritables mini-ordinateurs et il est maintenant bien plus facile de détourner ce genre d'appareils. Mais l'auteur oublie vite qu'il existe plusieurs marques différentes avec chacune leur système d'exploitation. Chaque système a ses spécificités et ses vulnérabilités.

L'auteur parle de la possibilité d'allumer l'appareil à distance. Ceci n'est possible que si l'appareil a été mis en veille ou si il possède un composant permettant de le mettre en route à distance. Hors ce dernier critère ne concerne qu'une faible minorité des appareils.

La conclusion nous vient d'ailleurs d'un internaute :

La plupart des téléphones ont [ sont dotés de programmes ] des softs que des barbouzes compétents pourraient adapter pour un usage d'espionnage, et avec la limite du problème de l'énergie disponible un portable peut faire un très bon micro espion. Il existe d'ailleurs des modèles particuliers de téléphone pour faire des mesures de qualité et des tests, il est probable (le contraire ne serait pas professionnel) que les services spéciaux aient commandé à des industriels spécialistes des contre mesures des téléphones adaptés à leurs missions (écoute, géolocalisation, etc.), de même que des dispositifs d'écoute et d'interception des communications sur mobile voire d'écoute de PC par les fréquences claviers/moniteurs. Enfin, même si les liaisons sont cryptées, l'interception d'une liaison radioélectrique n'est pas un problème avec la puissance de calcul dont on dispose aujourd'hui même sur un simple pc. Bref, une évidence qu'il faut rappeler tout ce qui est transmis par radio est potentiellement écoutable.

Un lecteur s'interroge sur la raison pour laquelle Ben Laden n'a jamais été localisé. Outre le fait qu'on ne soit pas certain qu'il vive encore, il n'utilise apparemment pas le téléphone cellulaire, ni aucune forme de moyen de communication radio électrique. D'après ce qu'on sait, les groupes style Al Qaïda sont revenus au système de la messagerie « parlée », comme dans l'Antiquité.

Un internaute nous révèle :

Et pour connaître des gens, vous pouvez aller à des conférences comme le CCC à Berlin, les témoignages d'ex-membres du MI-5 ou d'activistes surveillés sont plutôt convaincants.

Je doute que ça arrive à Mme Michu, par contre ça peut arriver à des personnes engagées politiquement. Et enlever la batterie c'est le B.A.-BA, avec l'achat de portable prépayé en liquide ou le clonage de carte SIM.

Un autre moyen d'éviter l'écoute consiste en effet à acheter un téléphone à carte pour un seul usage, très bref. Il sera toujours possible de localiser le lieu d'émission, mais trop tard pour l'exploiter.

Je vous invite à consulter mon article sur rue89, et surtout les commentaires. Le débt a pris trop d'ampleur pour que je l'ignore. J'ai répondu directement à certaines observations. Et je vous présente mes excuses pour l'aridité de cette réponse, probablement trop technique, rédigée grâce aux internautes.

## **ECOUTES - Polémique**

07 Dec 2008

Un prof pas content de mes informations sur les écoutes et interceptions de sécurité

Mon papier sur les nouvelles techniques d'écoutes a provoqué une avalanche de lectures et un début de polémique : sur rue89, pas moins de 44.000 visites uniques, ce qui est énorme. "Tu surfes sur les angoisses, me dit un de mes amis. Il est normal que les gens se précipitent dans cet entonnoir. Ainsi, un professeur d'électronique m'écrit, dans des termes pour le moins cavalier :

Je suis professeur en électronique et je suis attré par votre article. ETES-VOUS VRAIMENT JOURNALISTE ?

Oui, je suis vraiment journaliste. Mais il m'a fallu beaucoup d'efforts pour obliger ce "professeur" à l'orthographe totalement défailante à se dévoiler. Il ne m'en délivre pas moins une leçon magistrale.

Résumé de cours sur la téléphonie mobile :

#### EN MODE VEILLE :

Le mobile envoie des signaux de positionnement à l'opérateur qui permettent à celui-ci de savoir quelle antenne (BTS) est la plus proche de l'utilisateur afin d'obtenir une qualité optimale. Cette localisation permet aussi de passer d'une antenne à une autre sans coupure de la communication lorsque l'utilisateur se déplace (HANDOVER).

Cette technique fonctionne de la manière suivante :

- On mesure la puissance du signal transmis à plusieurs antennes BTS (au moins 3)
- On détermine la distance entre le mobile et chacune de ces antennes
- On utilise une technique similaire à la triangulation pour déterminer votre position

Elle peut être utilisée pour vous localiser MAIS CELA N'A RIEN A VOIR AVEC LE GPS (qui fonctionne à l'aide de satellites) ET sa précision est de 300 mètres et deux kilomètres (selon qu'on soit en zone dense/urbaine ou en zone rurale).

Pour ce qui est de l'écoute « ambiante ». Aucune procédure de ce type n'est prévue ni dans la norme GSM/GPRS/EDGE ni dans sa variante DCS ni dans la norme 3G/UMTS/HSDPA.

Pour que cela soit possible il faudrait que ces normes établies par le CEPT (European Conference of Postal and Telecommunications Administrations) soient volontairement falsifiées pour le grand public et que tous les acteurs du secteur soient dans le coup (une centaine de constructeurs et plus de 300 opérateurs dans le monde ainsi que toutes les sociétés sous-traitantes)

CA FAIT UN PEU TROP GROS COMME COMLOT, NON ?????

De plus avec du matériel de laboratoire il est également possible de mesurer les émissions GSM d'un mobile... Tous les électroniciens et bidouilleurs du monde sont dans le coup aussi !!! Vous vous rendez compte ....

#### EN MODE APPEL :

Il est tout à fait possible d'écouter les conversations !

BON je vous épargne le passage sur l'écoute lorsque le mobile est éteint...

ET le passage sur l'écoute lorsque le mobile est éteint et la batterie débranchée je préfère en rire...

Voici ma réponse, sans omettre de mentionner les innombrables fautes de grammaire et d'orthographe, étonnantes pour un prof !

Je ne doute pas de vos connaissances techniques, c'était d'ailleurs mon niveau de connaissances atteint il y a quelques semaines. Par exemple, la géolocalisation des appels par portable par triangulation utilisant les antennes de la cellule comme bases de calcul, technique utilisée notamment dans l'affaire Erignac. Mais elle nécessitait des émissions actives à un moment donné, répercutées par les opérateurs vers les enquêteurs. C'est un stade tout à fait dépassé. De nouvelles informations tirées de sources que je ne peux citer m'ont permis d'évoluer radicalement vers le niveau de connaissances évoqué dans mon papier. C'est évidemment perturbant. GPS : sur une question précise, mon interlocuteur m'a bien répondu que les techniques de géolocalisation étaient employées par l'intermédiaire des téléphones portables utilisées comme balises radio pour le "tracking volontaire", par les sociétés de transport. Interceptions téléphone fermé. J'aurais dû m'en douter en lisant les instructions données pour identifier les personnes qui volent des portables : même si vous changez de puce, même si vous enlevez la batterie, il semblerait que l'appareil lui-même soit porteur d'une identification électronique permettant de le repérer, je ne connais pas le détail exact. Mes connaissances étaient suffisantes et mon informateur bien identifié pour que je puisse considérer comme crédibles ces nouvelles informations. J'ajouterais ceci : des techniques de contrôle à distance sont systématiquement mises en œuvre dans le trafic internet, de très nombreuses "réparations" sont effectuées à distance ; les techniciens avec lesquels je travaille pour mon propre blog ne viennent jamais chez moi, ils se contentent de me poster un mail pour m'informer des travaux effectués. A fortiori, tout site internet, toute boîte de courrier est accessible à distance, et sans en informer

forcément l'utilisateur. Ce qui signifie en clair que toute votre messagerie peut être interceptée sans la moindre difficulté. Et même, au besoin, manipulée.

Une précision à propos de l'emploi éventuel des portables dont on aurait retiré la batterie pour éviter les interceptions. Je doute moi-même plus que sérieusement qu'il soit possible d'utiliser le portable dans cette configuration pour mener des opérations de tracking. Techniquement, il me semble en outre impossible que le portable sans énergie soit utilisable pour assurer des écoutes. Toutefois, selon certains techniciens, il apparaît que éventuellement, le portable soit susceptible d'être employé comme relais passif (micro dormant) dans certaines configurations. En tout état de cause, pour le moment, la plupart des techniques décrites ne peuvent actuellement être mises en oeuvre que par des techniciens de très haut niveau. Affirmons-le clairement, par des services de renseignement. Qui ont toujours été à l'origine des principales avancées en matière d'écoutes.