Les dossiers pratiques de Anonymat.org

Téléphonie

vie privée !

1ere Edition du 15 septembre 2000
Rev. 1.1

I.- Introduction

Le développement de la téléphonie et de ses annuaires a engendré des atteintes à la vie privée des utilisateurs du téléphone. Hier les annuaires imprimés, puis le Minitel© et les annuaires électroniques inversés, aujourd'hui le téléphone Wap, notre vie privée se réduit comme une peau de chagrin.
Dans ce dossier nous tenterons de vous proposer des contre-mesures afin de protéger, tant que faire se peut, votre vie privée mais également des informations pratiques sur la norme GSM.

II.- Téléphonie Filaire

La multiplication des annuaires imprimés, l'avennement du Minitel© et de son annuaire électronique puis le développement du marketing et jusqu'à une période récente, celui d'Internet sont autant de causes de multiplication de l'exploitation des informations nominatives concernant les abonnés du téléphone.

France Télécom (**FT**) fait commerce de ses fichiers qu'il revend à prix d'or aux entreprises interessées. Parallèllement les annuaires électroniques ont été victimes de pillages, à l'aide de programmes capables d'extraires les informations du Minitel© ou de l'Internet, afin de se constituer des fichiers à moindre coût.

Harcelé par les publicitaires puis par les e-marketeurs ou régies publicitaires en lignes, **France Télécom** à été contraint, par les associations de consommateurs ou par la **Cnil**, de proposer des garde-fous, et notamment des listes d'oppositions, certaines sont connues comme la liste rouge d'autres beaucoup moins car **FT** se garde bien d'en faire trop de publicité.

Les listes d'oppositions

La Liste Rouge

La souscription payante (env. 15 F/mois) à la Liste Rouge vous assure de ne pas paraître dans les annuaires de **FT** (notamment les Pages Blanches) et que vos coordonnées téléphoniques ne seront pas dévoilées par les opérateurs des centres de renseignement (le 12).

Sachez cependant que votre numéro de téléphone « secret » apparaitra quand même sur les écrans à cristaux liquides des téléphones des abonnés ayant souscrit un abonnement au service « **Présentation du Numéro** » et aux abonnés à *Numéris* (téléphone numérique a intégration de services) ainsi que par les Pompiers (18), le Samu (15), la Police (17), et l'Elysée.

Pour résoudre ce problème vous pouvez opter pour le *Secret Appel par Appel* (3651) avant chaque appel « confidentiel » ou pour le *Secret Permanent* (gratuit) afin de garder vos coordonnées secrètes (sauf services d'urgences).

La Liste Orange

Si vous ne souhaitez pas recevoir des publicités dans votre boîte aux lettres ou être démarché par le biais du téléphone, du telex ou de la télécopie, je vous conseille vivement de vous inscrire à la Liste Orange.

Cette liste gratuite vous assure de ne pas figurer dans les fichiers Marketing vendus par **FT**. Mais le « pompage » sauvage des annuaires téléphoniques du Minitel© par les entreprises rendait cette liste inutile : rien n'indiquait la présence ou non à la liste orange. Depuis peu, **FT** a été contraint de placer un marqueur (en fait une astérix) sur les pages de ses annuaires électroniques, en face de chacun des abonnés qui ont souscrit à la liste orange et les entreprises contraintes de ne pas importuner ces personnes sous peine de poursuites.

Vos coordonnées pourront cependant être transmises par les opérateurs des centres de renseignements (le 12) et apparaitront dans les annuaires.

Les abonnés à la **Liste Rouge** sont automatiquement à la liste Orange.

La Liste Safran

La Liste Safran (gratuite) est une liste Orange pour les télécopieurs (fax) et les télex, à destination des professionnels. Vos numéros de télécopie et télex ne seront pas divulgués à des fins Marketing.

Ils seront néanmoins présents dans les différents annuaires imprimés et électroniques de **FT** et pourront êtres transmises par les opérateurs du 12.

La Liste Chamois

Avec la Liste Chamois vos numéros de télécopie et télex ne paraitront pas dans les annuaires imprimés et électroniques de **FT**. Mais ils pourront être transmis par les opérateurs de centres de renseignements comme le 12.

Vos coordonnées seront identifiées si vos correspondants sont abonnés à *Numéris* ou à la formule « *Présentation du Numéro* », également par les Pompiers (18), le Samu (15) ou la Police (17), ainsi que l'Elysée.

Comme pour la Liste Rouge vous pouvez opter pour le *Secret Appel par Appel* (3651) ou le *Secret Permanent* afin de garder vos coordonées secrètes (sauf services d'urgences).

Secret Permanent ou Appel par Appel

Pour éviter l'affichage de votre numéro de téléphone chez votre correspondant , vous avez deux solutions :

- Soit « masquer » chaque appel confidentiel en tapant la séquence « **3651** » avant le numéro de téléphone de votre correspondant.

- Soit opter pour le « Secret Permanent », gratuit, pour ne jamais dévoiler votre numéro.

Sachez que le masquage ne fonctionne pas pour les services d'urgences (Pompiers, Police, Samu) ainsi que pour l'Elysée.

A noter : l'abonnement au *Secret Permanent* (anciennement appelé *Liste Ivoire*) entraine une incapacité de jouer à certains jeux téléphoniques notamment ceux issues des émissions de télévision ou radiophonique, qui utilisent votre numéro de téléphone pour vous identifier (voir la section suivante).

Les annuaires inversés

Ce sont des annuaires de recherche qui permettent de retrouver le nom et l'adresse d'un correspondant à partir de son numéro de téléphone ou de fax.

Le plus connu et le premier annuaire de recherche inversé est le **3617 ANNU** (5,57F la minute) du groupe télématique Iliad qui détient également le fournisseur d'accès Internet Free.

France Telecom vient de mettre en ligne son propre annuaire de recherche inversé sur le **3615** (2,23F/min) **et 3617 QUIDONC** ou le 08 36 68 01 11 (vocal)

Un **3615 LANNUAIR** est également en service d'après l'annuaire du téléphone.

Ces annuaires sont une atteinte à la vie privée et au droit à l'anonymat car toute personne qui donne son numéro de téléphone peut être localisée sans son accord, même involontairement car votre numéro s'affiche sur le combiné de votre correspondant qui peut effectuer une recherche inverse et connaître ainsi l'appelant.

Ces techniques sont d'ailleurs utilisées par de nombreuses sociétés qui recueillent les numéros des appelants pour se constituer des fichiers nominatifs à des fins Marketing, sans que vous ne vous en rendiez compte !

La **Cnil** à prévu un droit d'opposition à ce mode de recherche, que je vous conseille vivement de faire valoir auprès de votre agence **France Télécom** ou en appelant le numéro vert suivant :

0 800 55 97 02

Une confirmation écrite vous sera adressée sous quelques jours.

Pour le **3617 ANNU** appelez le **01 56 26 20 00** pour vous mettre en opposition, si vous passez par le 3617 faites vous rembourser la communication, c'est votre droit.

Pour chaque annuaire inversé un numéro gratuit d'opposition est mis à la disposition du public. Seule contrainte : il vous faudra faire la démarche pour chaque service auprès duquel vous souhaitez vous faire « interdire ».

Enfin, certains sites pornographiques facturent jusqu'à 900FF de l'heure en vous identifiant grace à l'affichage de votre numéro de téléphone puis en retrouvant vos coordonnées dans un annuaire inversé afin de vous envoyez la facture à votre domicile. Sachez que ce procédé est illégal et que vous pouvez refuser de payer.

Les annuaires sur le Web

Les annuaires se déplacent sur le Net et leur multiplication risque de poser de nombreux problèmes. On m'a communiqué l'adresse d'un site *underground* qui présente un annuaire des abonnés à la Liste Rouge ! Bien sur, je ne le rendrais pas public car ce n'est pas l'objet de ce dossier, bien au contraire.

FT a fait migrer son annuaire électronique (3611) sur l'Internet. Ainsi l'on retrouve les fameuses *Pages Blanches* des particuliers et *Pages Jaunes* des professionnels.

Parallèlement une « *Liste Anti-Web* » a été mise en place par **France-Télécom** pour ceux qui ne souhaiterait pas apparaître sur les annuaires Internet de **FT** : appelez le numéro vert suivant :

0 800 77 44 03

Une confirmation écrite vous sera adressée sous quelques jours.

Des sites portails vers les annuaires de nombreux pays sont en fonctionnement comme infobel qui propose les annuaires téléphoniques de la France, Belgique, Luxembourg, USA, Espagne et Danemark et une recherche de l'abonné à partir de son téléphone.

Bloquez les appels malveillants !

Un nouveau service payant (25 F/mois) de **France Télécom** nommé « *bloquage des appels malveillants* » ou **BAM** permet de bloquer les appels de personnes que vous trouvez indésirables.

Ces personnes sont identifiées par leur numéro de téléphone et si l'une d'elle à masquée son numéro ou est au « Secret Permanent » empèchant le fonctionnement du « filtre », elle tombera sur ce message : « Votre correspondant a demandé que les appels avec Secret du numéro ne lui soit pas transmis. Merci de renouveler votre appel en autorisant la présentation du numéro ou en appelant depuis une autre ligne si vous êtes abonné au Secret Permanent. »

Nous voyons une fois de plus que **FT** fait marche arrière, sous certaines pressions, pour inciter les abonnés à ne pas se mettre au Secret Permanent ou a masquer leur numéro.

III.- La Téléphonie GSM

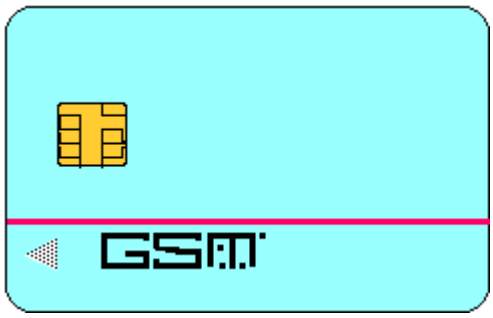
La téléphonie GSM pose de nombreux problèmes, outre les problèmes de santé lié à l'émission d'ondes électromagnétiques intenses près du cerveau, ainsi qu'aux émetteurs surpuissants présents sur les immeubles (voir le site Scandales Français et le chapitre « des chercheurs ont peur »), les problèmes mettant en cause la vie privée de ses utilisateurs font froid dans le dos et ne font que commencer.

Les principes techniques

La signification du sigle **GSM** est : *Global System for Mobile Communications*, c'est à dire Standard pour un système commun de téléphonie cellulaire numérique. Le **GSM** est un système de télécommunication radio. La principale application aujourd'hui est la téléphonie mais il peut aussi être utilisé pour de la transmission de données (9600 bds maximum) ou pour l'envoi de messages courts (**SMS**). Il constitue également un réseau sécurisé qui assure la confidentialité des communications.

Définissant les procédures de transmission cellulaire numérique, le **GSM** permet à des appareils de plus en plus petits d'effectuer des appels avec une qualité proche du filaire. Il assure aussi la confidentialité rendant quasiment impossible l'écoute clandestine. C'est une carte à puce appelée **SIM** (Subscriber Identity Module) qui tient lieu de ligne téléphonique. Elle est dissociée de l'appareil lui-même. Il lui suffit de la glisser dans un terminal **GSM** quelconque (pas forcément le sien), puis de composer son code personnel pour obtenir sa communication.

La carte **SIM** (*Subscriber Identity Module*) contient l'ensemble des caractéristiques de l'abonnement y compris l'identité de l'abonné. C'est une carte à puce à microprocesseur qui s'insère dans le terminal. Elle permet d'authentifier l'abonné.



La carte **SIM**.

Le téléphone mobile fonctionne au moyen de signaux radios qui transitent via des émetteurs (BTS) souvent installés en haut d'immeuble dans les villes. Chaque émetteur représente une cellule. La France est divisée en cellules dont la taille varie de 50m à 10km.
Les techniques de localisation utilisent soit le **GPS** qui repose sur les satellites, soit la triangulation du réseau **GSM** : un utilisateur se trouve toujours dans une cellule principale et est couvert par deux autres, ce qui permet d'éviter les coupures de communication en cas de déplacement. On détecte où se trouve l'abonné en recoupant

les informations qui proviennent de ces trois cellules. C'est la méthode choisie par les forces de police quand elles enquêtent sur commisssion rogatoire. L'inconvénient est le manque de précision, surtout en province où les cellules atteignent parfois 30 km.

Les enjeux

La localisation est donc le principe de base du fonctionnement de tout téléphone mobile. Cependant cette localisation peut se transformer en pistage.

La *publicité localisée* ou **SMSCB** est déjà en phase de test. De quoi s'agit-il ? Un message publicitaire est posté sur une cellule à tous les utilisateurs de mobiles se trouvant dans la zone concernée. En clair, cela signifie que lorsque vous passerez devant une grande surface, celle-ci pourra envoyer des « informations » publicitaires, par exemple une promotion, à tous les utilisateurs de mobiles se trouvant à proximité (et jusqu'à 10 km à la ronde !) de son magasin. Le canal Promotion de SFR est prévu pour cette année.

Il y a également la publicité nommée « Push », qui utilise des messages SMS (*Short Message Services*), des messages de services courts qui s'affichent sur le mobile des abonnés qui ont préalablement et docilement livrés à leur opérateur des informations personnelles pour les « profiler » !

Toutes ces techniques sont basées sur un impératif : le repérage des utilisateurs de mobiles. Et c'est la que le bas blesse. Avec l'évolution de la technologie un utilisateur de mobile sera bientôt pisté à 10 mètres près !

La **Cnil** (Commission nationale de l'informatique et des libertés) a une position claire : « On ne peut pas aujourd'hui, ne pas être localisé car c'est le propre de la téléphonie mobile. » Toutefois pour une utilisation commerciale des informations de localisation il faut montrer patte blanche et présenter un dossier à la **Cnil**. Certains opérateurs ont déjà déposé leur candidature. Et la Cnil de réfléchir à de nouveaux droits : « Pourquoi ne pas garantir au public le droit à l'injoignabilité, à être branché sans être localisé. ». Du côté de l'**ART** (*Régulation des Télécommunications*) on penche pour le bon sens : l'utilisateur ne souscrira pas à l'option *localisation* s'il ne veut pas être localisé.

Mais ce n'est pas aussi simple que cela, il suffit que vous donniez votre accord une seule fois, par exemple pour connaître le cinéma le plus proche d'où vous êtes, pour être localisé définitivement !

Reste la solution de listes d'oppositions comme le « Secret Permanent » (ex. Liste Ivoire).

D'après les opérateurs la localisation d'une personne ne sera jamais continue… C'est sans compter sur une société nommée CellPoint, leader dans les services de localisation cellulaire, qui à lancé un pavé dans la marre au mois de février 2000, en dévoilant à l'occasion du Salon GSM 2000 de Cannes un service de localisation pour le grand public nommé **Finder**.

Finder permet d'afficher sur l'écran de son mobile ou de son ordinateur, la distance qui vous sépare d'un ami, d'un collègue ou d'un conjoint qui possède un téléphone GSM. La réponse peut s'afficher graphiquement sur une carte si le téléphone est relié à l'Internet (téléphone Wap).

En conservant l'historique des localisations successives il devient facile de pister une personne. Un moyen d'espionnage à la portée de tous, d'autant qu'il suffit de donner son accord une seule fois pour être suivi par **Finder** !

Les risques sont d'autant plus grand que le prochain standard successeur du **GSM Data**, le **GPRS**, prévu pour la deuxième moitié de l'an 2000, permettra outre un débit beaucoup plus important (171 Kbps) une connection permanente propice à la « filature électronique », avec une facturation des services au volume des données échangées donc indépendamment du temps de connexion.

Le téléphone Wap ajoute aux possibilités de pistage propre à la technologie GSM les risques inhérents à l'Internet.
Ainsi un américain a découvert qu'en faisant des achats sur le Web (chez Amazon.com) à l'aide de son téléphone Wap, son numéro de téléphone était communiqué aux sites Web qui en faisaient la demande. Rien n'empêche de penser que cette pratique est courante chez les fournisseurs d'abonnement téléphonique (ici, Sprint) qui disposent de toutes les informations générées par les connexions et la navigation des utilisateurs.

France Télécom planche sur un système permettant une traçabilité parfaite des usagers du téléphone : attribuer un numéro unique à chaque abonné. **La Poste** de son côté instaure une adresse électronique gratuite et permanente à chaque français « qui en fera la demande ». Comme on le voit tout est mis en place pour faciliter l'identification des usagers, peut-être faut il y voir la main mise des Services Secrets pour lesquels ces mesures facilitent considérablement les interceptions de sécurité.

En angleterre une société, Starium, présente un produit contre Big Brother, un boîtier de chiffrement, de la taille d'un Palm, qu'il suffit de brancher entre une prise téléphonique et le combiné pour un prix d'environ 700F. Ce produit qui utilise les algorithmes Diffie-Hellman et Triple-DES serait commercialisé en France. Une première, si les autorités autorisent sa commercialisation.

Le Service de messages courts (SMS)

Vous pouvez envoyer un message court, aussi appelé télémessage ou mini-message, à destination d'un mobile afin de ne pas déranger son propriétaire par exemple ou ne pas être intercepté par sa messagerie.

Des sites Web proposent l'envoi de messages gratuits de 160 caractères maximum soit 4 lignes de texte. Depuis votre PC connectez vous sur un de ces sites :

- SMSgratuit 3 messages gratuits par jour.
- Kiwee 15 messages gratuits par jour.
- Everyday.com 10 SMS par jour.
- Mobimel seulement 2 messages/jour…
- Cerclo Un des pionniers du SMS gratuit jette l'éponge ! (a lire)

Votre opérateur téléphonique peut proposer également ce genre de service comme www.SFR.com.

A noter : les caractères accentués ne sont pas toujours pris en compte ni les pièces jointes.

Les codes « Secrets » du GSM !

Pour la constitution de mon dossier, j'ai appelé le « Service Client » de France Télécom Itinéris en leur demandant les différentes combinaisons de touches pour accéder aux différents services des GSM. Devant mes questions techniques (saugrenues ?) j'ai été aimablement aiguillé vers le « Service Commercial ». Ce dernier, et après consultation d'un interlocuteur sans doute hiérarchique (un blanc géné puis… patientez quelques instants.) m'a éconduit en affirmant « ne pas vouloir me donner ce genre d'information ! »

Incroyable ! Connaître les numéros à composer pour utiliser leurs services (parfois payants) relève du secret d'état ! Divulguer le code à composer pour masquer ou démasquer son numéro est « confidentiel défense » chez France Télécom ! et cela s'appelle un service public !

Il est vrai que dans leur agence commerciale, pas un seul prospectus sur le sujet ! même les vendeurs ne sont au courant de rien ! heureusement que sur Internet l'information est plus prolixe sur le sujet…

Voici présenté sous forme de Questions-Réponses les principaux codes qui concernent, dans le cadre de ce dossier, la sécurité ou la protection de son anonymat :

Q : Comment obtenir le numéro d'identification (IMEI) de mon portable ?

Eteindre le mobile, le rallumer, ne pas composer le code SIM mais ***#06#**

Ce code unique à 15 chiffres, de format XX-XXXX-XX-XXXXXX-X, est indiqué sur l'appareil (souvent sous la batterie) et est également stocké en mémoire.
A noter que **FT** à la possibilité d'inactiver le combiné à distance, à l'aide de ce numéro, en cas de vol, ce qu'il fait rarement…

Q : Comment savoir si mon portable, acheté d'occasion, a été volé ?

Vérifiez que son numéro d'identification (IMEI) correspond bien à l'étiquette collée au dos du mobile, dans le cas contraire cela pourrait être un téléphone volé.

Q : On m'a parlé d'un Menu caché contenant diverses informations « confidentielles ». Est-ce vrai ?

Effectivement, ce menu est accessible en tapant le code ***#92702689#** ce qui correspond aux lettres ***#WAR ANTY#**.

Il affiche un menu destiné à la maintenance de votre portable :

-1. Numéro d'identification IMEI
-2. Mois et année de production
-3. Date d'achat (à rentrer soi-même une fois pour toute !)
-4. Date de réparation
-5. Transfert de données
-6. Cumul du temps passé avec le portable (sur certaines versions)

Q : Puis-je masquer mon numéro à mon correspondant ?

Tout à fait ! Vous pouvez masquer votre numéro afin que votre correspondant ne puisse pas visualiser votre numéro de portable.

Pour masquer systématiquement votre numéro tapez la séquence **#31#**
Pour masquer ponctuellement votre numéro au destinataire tapez **#31#numéro**

Pour montrer sytématiquement votre numéro tapez ***31#**
Pour montrer ponctuellement votre numéro tapez ***31#numéro**

Pour consulter l'état masqué ou démasqué tapez ***#31#**

Q : A contrario, Puis-je voir le numéro de mes correspondants ?

Encore gagné ! pour voir les numéros des appelants tapez ***30#**
pour ne plus les voirs tapez **#30#**
Enfin, pour consulter l'état : affichage ou non, tapez ***#30#**

Q : J'ai saisis trois fois un mauvais code PIN ! comment débloquer mon appareil ?

Le code **PIN** (Personal Identification Number) est utilisé pour protéger la carte SIM (vous me suivez ?). par défaut il est demandé à chaque mise sous tension du terminal, avant de pouvoir utiliser la carte SIM.

Le bloquage peut rendre la carte SIM inutilisable. Le code doit être débloqué en utilisant un code **PUK** (PIN Unblocking Key) - vous êtes toujours là ? bon ! on continue…
Pour obtenir ce dernier code contacter votre opérateur. Une fois en possession de ce code composez :

****05*CodePUK*nouveauPIN*nouveauPIN#**

Astuces avancées

Les manipulations décritent ci-dessous ne sont pas recommandées par les opérateurs téléphoniques. Ils se font à vos risques et périls… Nous déclinons toute responsabilité, etc.

Le Dévérouillage ou Sim Lockage

Merci au site www.ifrance.com/nokiafun/

Les portables achetés en magasin sont vérrouillés électroniquement sur 4 ports (4 verrous) afin d'éviter les échanges de carte SIM avec les portables.

Les 4 ports sont :

1.- Bloquage sur la série de la carte Sim

2.- Bloquage sur le réseau

3.- Bloquage sur le pays d'origine de la carte Sim

4.- Bloquage sur la carte Sim elle-même

Code : #pw+nnnnnnnnnn+x#

Les lettres **p** et **w** s'obtiennent en appuyant successivement sur la touche *
Les 10 lettres « **n** » correspondent au **Master Code** de 10 chiffres.
La lettre « **x** » correspond au numéro de Sim-Lockage (Lock = verrou).

Le « Master Code » se calcul d'après le numéro de l'opérateur et le numéro d'IMEI (que nous avons vu plus haut).

Pour « contrôler » les verrous (ou ports) de votre portable vous devez taper un numéro Master Code bidon de 10 chiffres (ex : 0123456789)

Pour contrôler le Sim Lock (port) numéro 2 tapez : #pw+0123456789+**2**#

Si un message de type « SIM WAS NO RESTRICTED » s'affiche sur votre portable, c'est qu'il n'est pas vérrouillé sur le port 2. Si au contraire il affiche le message « CODE ERROR » c'est que le port 2 est vérrouillé.

Attention toutefois, au bout de 3 ou 4 tentative de contrôle d'un port, le portable pourrait-être susceptible de se bloquer !

Quelle est l'intérêt de cette manipulation ? Si tous les ports sont dévérrouillés vous pouvez mettre n'importe qu'elle carte SIM dans votre portable, provenant de n'importe quel opérateur !

Théoriquement, votre opérateur doit vous fournir un code de déverrouillage au bout de 6 mois. Contactez le.

Pour ceux qui n'arrivent pas à débloquer leur mobile, des portables d'occasions dévérouillés sont disponibles sur les sites d'enchères en ligne…

Dévérouillage occasionnel

Pour utiliser occasionnellement une carte SIM d'un opérateur différent sans avoir à modifier les ports ou verrous, il existe une astuce :

- Insérer la nouvelle carte
- Allumez le portable
- Pressez la flèche haut pendant 3 secondes
- Puis pressez la touche « c », pressez « * » jusqu'à ce que l'écran réapparaisse, recommencez,
- Tapez la séquence 04*CodePIN*CodePIN*CodePIN#

Si la manipulation a réussie, le portable doit afficher « Code Pin Change ».