1 LE SYSTÈME GSM

L'utilisateur d'un téléphone portable ne réalise généralement pas qu'il se trouve en prise directe avec ce qui est peut-être le système le plus complexe jamais créé par l'homme : le réseau mondial de télécommunications. On qualifiait déjà ainsi le réseau téléphonique international il y a une vingtaine d'années, avant qu'il ne s'imbrique inextricablement avec Internet et les systèmes de communication mobile, terrestres ou satellitaires.

Il est édifiant de méditer cet avis d'un expert, qui estime que la mise sur pied du seul système de téléphonie mobile GSM aurait nécessité environ dix fois plus d'efforts qu'il n'en a fallu pour qu'un homme pose le pied sur la Lune... Et pourtant, le téléphone portable est aujourd'hui le produit « grand public » par excellence, incroyablement peu coûteux et extrêmement simple à utiliser.

Si l'emballement du nombre d'utilisateurs ne date vraiment que de la fin 1998, voire de l'année 1999, l'aventure du GSM trouve son origine vers les années quatre-vingt, soit près de vingt ans en arrière ! Souvenons-nous : le téléphone de voiture était alors un luxe ruineux, outil de travail ou gadget, mais réservé en tout cas à une élite fortunée. En tout état de cause, les techniques utilisées à l'époque n'auraient jamais supporté la démocratisation de la téléphonie mobile telle qu'elle se confirme depuis quelques années, car la saturation des fréquences menaçait déjà.

C'est dans notre vieille Europe, et tout particulièrement en France, que quelques précurseurs ont su anticiper ce phénomène, à peu près au moment où Roland Moreno inventait la carte à puce. Ce n'est peut-être donc pas tout à fait un hasard si le téléphone portable, tel que nous le connaissons, doit une bonne partie de ses possibilités à une carte à puce, la carte « SIM ».

1.1 UN PEU D'HISTOIRE

Transportons-nous donc au début des années quatre-vingt. À cette époque, la téléphonie mobile reposait sur des techniques largement analogiques, encore que déjà « cellulaires ». Chaque pays avait développé son propre réseau (RADIOCOM 2000 en France), strictement national car n'offrant aucune inter-opérabilité aux abonnés des réseaux étrangers.

À l'heure où nous écrivons ces lignes, ces réseaux ferment les uns après les autres, libérant ainsi des bandes de fréquences qui ne tarderont pas à être réemployées de façon infiniment plus efficace et plus sûre.

À vrai dire, c'est probablement l'ampleur des investissements de recherche et développement à prévoir qui a poussé, à l'origine, à mettre sur pied une collaboration internationale. Celle-ci s'est tout d'abord organisée sous l'égide de la CEPT (Conférence des administrations Européennes des Postes et Télécommunications), à la suite d'une étude franco-allemande sur l'avenir (préoccupant !) des radiocommunications mobiles. En 1982, cette instance réunissait 26 pays européens, ou plutôt leurs administrations des PTT respectives. Bien qu'encore presque toutes organisées sous la forme de monopoles étatiques, ces dernières ont pourtant su comprendre que le bénéfice évident d'une coopération pan-européenne devait prévaloir sur les intérêts nationaux qu'elles avaient plutôt l'habitude de protéger bec et ongles.

C'est ainsi que fut créé, au sein de la CEPT, le « Groupe Spécial Mobile » dont les initiales (GSM) devaient ultérieurement devenir celles de *Global System for Mobile communications*. Sa mission : développer les spécifications d'un réseau véritablement pan-européen, capable d'accueillir des abonnés par millions, et non plus par milliers, tout en se jouant des frontières. Vaste programme, assurément, riche de difficultés techniques, économiques, et logistiques à la hauteur des enjeux dont nous récoltons aujourd'hui les fruits.

Après la reconnaissance du GSM par la Commission Européenne en 1984, la France, l'Italie et l'Allemagne signèrent un accord de coopération dès 1985, rejoints par le Royaume-Uni en 1986. Il était déjà bien clair que le système à mettre sur pied serait digital, complémentaire du RNIS (Réseau Numérique à Intégration de Services), et qu'il opérerait dans la bande des 900 MHz, deux plages de 25 MHz y étant d'ors et déjà réservées. Mais il manquait encore une volonté politique permettant de rassurer les fabricants de matériel, sans lesquels rien ne pouvait naturellement se faire.

Sous la pression de la France et de l'Allemagne, une réunion tenue en décembre 1986 devait déboucher sur une recommandation et une directive européennes, visant au lancement effectif d'un bouquet limité de services avant 1991. Le déploiement complet dans les métropoles européennes devait suivre avant 1993, la continuité entre ces zones devant devenir une réalité courant 1995. C'est également en 1986 que le GSM prit la responsabilité globale (et redoutable !) de la coordination du développement de l'ensemble de la spécification.

Restait à associer efficacement à l'aventure les opérateurs potentiels, autrement dit les futurs constructeurs et exploitants de réseaux. Ce fut chose faite dès septembre 1987, avec la signature à Copenhague, par des opérateurs de treize pays, du MoU ou

Memorandum of Understanding, l'équivalent en somme d'une ferme déclaration d'intention en faveur du projet.

Entre-temps, les tests de validation de huit ou neuf options différentes en matière de transmission radio avaient déjà commencé, en France, avec pour principal résultat le choix indiscutable de la technologie TDMA (*Time Division Multiple Access*), autrement dit du multiplexage temporel.

Notons que le CNET (l'organe de recherche de ce qui devait devenir France Télécom), joua un rôle tout à fait prépondérant dans sa mise au point.

En février 1988, la faisabilité du système était suffisamment démontrée pour que tous les opérateurs signataires du MoU soient officiellement invités à faire acte de candidature. Il ne restait « plus qu'à » mener à bien un immense travail de développement et de test des spécifications définitives, appelées à franchir le cap (provisoire !) des 6 000 pages en 1997… L'ampleur et la complexité de ce travail de bénédictin se révélèrent vite telles que la date de lancement du service, fixée au 1er juillet 1991, risquait fort de ne pas pouvoir être tenue. Il fut donc décidé de scinder le projet en deux phases mutuellement compatibles, afin de pouvoir lancer, dans les délais impartis, un système incomplet mais néanmoins fonctionnel.

Le transfert de responsabilité, en 1989, du GSM à l'ETSI (*European Telecommunications Standards Institute*, nouvellement créé à Sophia-Antipolis en France), vint heureusement activer les choses en accentuant la coopération entre administrations, opérateurs, et industriels, tous placés pour une fois sur un pied d'égalité. La « Phase 1 » de la spécification GSM put ainsi être publiée dès 1990, et adoptée *in extremis* pour le système à 1 800 MHz imaginé entre-temps en Angleterre, l'ancêtre en somme du DCS 1800 rebaptisé depuis GSM 1800. Hélas, seul un réseau pilote put être présenté au salon TELECOM 91 à Genève… Cela pour la bonne et simple raison qu'à cause de sombres questions d'agrément, il n'y avait pas encore de téléphones GSM sur le marché ! Il faut dire que les téléphones GSM ont été parmi les tout premiers équipements de télécommunications à bénéficier d'un agrément européen unique, et non plus délivré pays par pays. Or, les procédures d'agrément n'étaient tout bonnement pas prêtes en 1991…

Ce n'est finalement qu'en avril 1992 qu'une procédure d'agrément provisoire rendit possible la commercialisation massive des premiers « portables », stimulant immédiatement le dynamisme des opérateurs. Tout était en place pour qu'un effet de « boule de neige » se déclenche, et ne puisse plus être arrêté !

Dès juin 1992, le premier accord d'itinérance (*roaming*) était signé, permettant aux abonnés anglais d'utiliser leur portable en Finlande, et vice-versa : le réseau pan-européen était bel et bien sur ses rails.

Fin 1993, on comptait plus d'un million d'abonnés (contre plus de 700 millions début 2001 !), mais surtout le phénomène débordait de son cadre européen pour entreprendre la conquête du monde entier : l'opérateur australien Telstra rejoignait en effet les autres membres du MoU.

Aujourd'hui, la seule France a dépassé la trentaine de millions d'adeptes (soit un « taux de pénétration » proche de 50 %), que se partagent (plus ou moins équitablement !) trois opérateurs. Les mobiles GSM sont utilisables indifféremment dans quelque 120 pays de par le monde, et même les portables « satellite » fonctionnent selon la norme GSM.

À la phase 1 succéda rapidement la phase 2, et nous en sommes maintenant à la « phase 2+ » et son fameux STK (SIM Toolkit). Précurseur de la « troisième génération » de mobiles, le WAP (*Wireless Application Protocol*) est déjà talonné par le GPRS, en attendant l'UMTS et la complète intégration avec Internet !

Le marché est excessivement concurrentiel, pour le plus grand bénéfice du consommateur qui, pourvu qu'il fasse preuve d'une vigilance sans faille et d'un minimum de hardiesse, peut profiter de possibilités tout à fait extraordinaires à des prix dérisoires.

L'un des buts de cet ouvrage est précisément de lui montrer comment aller le plus loin possible dans cette voie…

1.2 LES NORMES GSM ET L'ETSI

Comme nous venons de le voir, c'est désormais l'ETSI qui est en charge de toute la normalisation relative au système GSM, et notamment de la publication des différentes parties de la spécification GSM.

À l'exception notable des informations détaillées sur les mécanismes sécuritaires (en particulier les algorithmes cryptographiques), qui ne sont en principe dévoilées qu'aux opérateurs et industriels signataires d'un engagement de confidentialité, il faut savoir que ces documents n'ont strictement rien de secret. Chacun peut en consulter le catalogue, passer commande, ou même procéder sous certaines conditions à leur téléchargement gratuit, sur le site internet de l'ETSI (http://www.etsi.org). Tous droits de reproduction et de communication sont toutefois réservés, selon les règles de droit commun en matière de propriété intellectuelle.

Le présent ouvrage ne saurait bien évidemment se substituer à tout ou partie de la spécification GSM, qui demeure la seule et unique référence officielle. L'auteur s'y est cependant très souvent référé lors de l'accomplissement de son travail, ainsi qu'à un certain nombre de sources d'information beaucoup plus officieuses, disponibles sur Internet.

Le lecteur désireux de pousser encore plus loin son exploration du système GSM est naturellement invité à faire de même, en commençant par étudier en détail l'incontournable norme GSM 11.11 puis en soumettant le sigle GSM à quelques bons « moteurs de recherche ».

Bien entendu, la spécification GSM n'est nullement figée, et d'importants travaux sont en cours pour préparer les prochaines générations de « communicateurs » mobiles, dont la téléphonie ne constituera sans doute plus qu'une bien petite partie des possibilités…

1.3 UN RÉSEAU NUMÉRIQUE

La grande innovation du GSM par rapport à la génération précédente de téléphones mobiles est le caractère entièrement numérique (ou digital) du système. Outre une utilisation infiniment plus efficace de cette ressource rare qu'est le spectre radioélectrique, cela évite que les communications puissent être écoutées par le premier radio-amateur venu, voire par n'importe quel simple curieux équipé d'un « scanner ».

Il faut toutefois savoir que la norme prévoit expressément des moyens d'écoute à l'usage des autorités judiciaires ou de police, et que l'on murmure dans les milieux universitaires que le décryptage non autorisé ne serait pas si compliqué qu'on veut bien le dire…

L'architecture numérique du système permet aussi la mise en œuvre de fonctionnalités très riches, parfaitement hors de portée des systèmes analogiques.

À vrai dire, il faut considérer le réseau GSM comme un « RNIS sans fil », autrement dit comme une version mobile de ce qui, en France, s'appelle Numéris. Ce n'est donc certainement pas une coïncidence si le nom de baptême du réseau GSM de France Télécom est Itinéris !

Le réseau GSM se prête ainsi à merveille à la transmission, en plus de la parole, de toutes sortes de données informatiques : messages écrits, télécopies, trafic internet, etc.

Le plus simple des téléphones portables renferme ainsi un véritable micro-ordinateur, dont la puissance est à la hauteur de la complexité et de la rapidité des tâches qu'il lui faut prendre en charge. Associé à une carte à puce (dite « SIM »), il apporte un niveau inégalé de sécurité, alors qu'on sait à quel point les systèmes analogiques étaient vulnérables aux tentatives de fraude.

La qualité du son a également tout à gagner d'une transmission purement numérique, même s'il nous faut dès maintenant tordre le cou à certaines croyances largement propagées par les publicités des opérateurs et des fabricants de téléphones :

- Même de très bonne qualité, le son d'un téléphone portable ne peut en aucune façon rivaliser avec celui d'un *compact disc*. Au mieux, il sera équivalent à celui d'un bon téléphone filaire.
- Par définition, le son d'un téléphone portable GSM est toujours numérique, et même s'il existe différents niveaux de qualité (dont la « haute résolution »), cela n'a techniquement aucun sens de laisser entendre que certains modèles bénéficieraient d'un « son digital » et d'autres pas.
- Une transmission numérique n'est pas soit parfaite, soit impossible : elle peut souffrir de toutes sortes de défauts, très différents il est vrai de ceux d'une transmission analogique (on constatera plutôt des échos, des coupures, ou des déformations, que du souffle ou des parasites).

Enfin, il faut savoir que les perturbations pouvant éventuellement être apportées dans le voisinage des matériels (postes mobiles ou stations fixes) en fonctionnement, sont fort différentes de celles imputables aux équipements d'émission analogiques.

1.4 UN RÉSEAU CELLULAIRE

Le secret de l'énorme capacité des réseaux GSM réside dans la combinaison de deux techniques très particulières :

- la transmission numérique à multiplexage temporel TDMA ;
- la structure « cellulaire ».

Cette dernière n'est pas une invention récente, puisque ayant fait l'objet dès 1947 d'un brevet déposé par Bell Laboratories... Entre-temps, les réseaux analogiques de téléphonie mobile en ont d'ailleurs largement fait usage.

La structure cellulaire est sans doute ce que l'on pouvait imaginer de plus astucieux pour s'accommoder, sur une zone géographique donnée, de l'éternelle pénurie de fréquences radio. L'idée

consiste à ce que la portée des stations fixes soit très limitée, de façon à ce que les fréquences qu'elles utilisent puissent être réemployées un peu plus loin, pour desservir d'autres abonnés sans risques d'interférences. Le revers de la médaille est, naturellement, que pour couvrir une zone donnée, il faudra d'autant plus de stations fixes que leur portée sera faible.

La **figure 1.1** schématise ce principe, en prenant pour exemple une zone dans laquelle onze « cellules » sont desservies par seulement quatre fréquences (A, B, C, D).

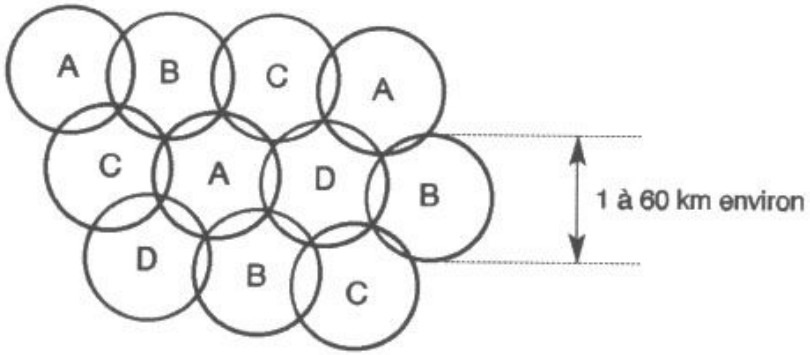


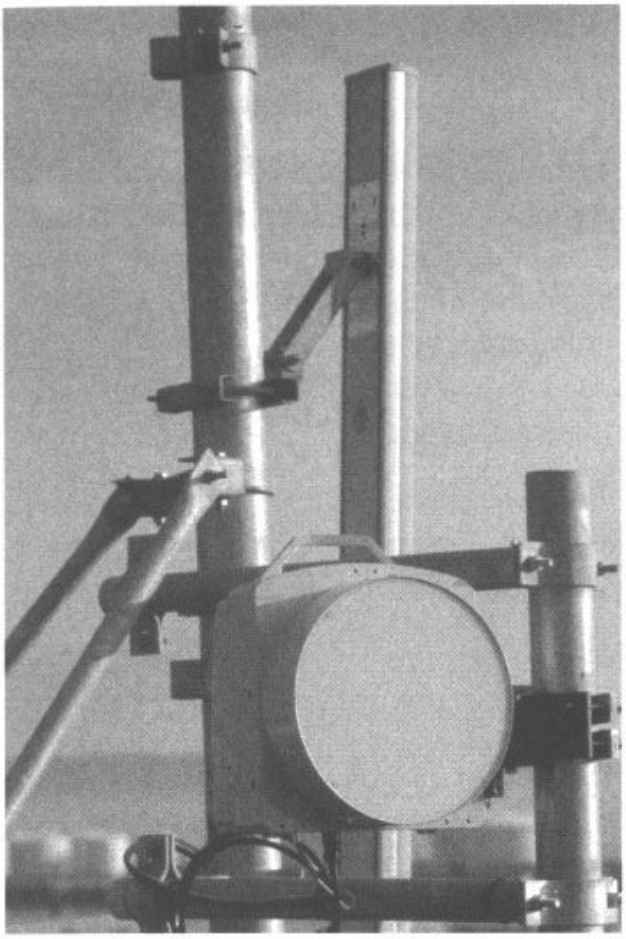
Figure 1.1.
Le principe d'un réseau cellulaire.

En pratique, les choses sont toutefois plus complexes, car il faut tenir compte de multiples impératifs tels que le recouvrement partiel des cellules, la proximité de stations fixes des réseaux concurrents, le relief du terrain, son degré d'urbanisation, etc. Tout cela mène à des diamètres de « cellules » qui peuvent, grosso modo, varier de quelques centaines de mètres en centre ville, à quelques dizaines de kilomètres en rase campagne.

Bien entendu, toutes les stations fixes d'un réseau cellulaire doivent être interconnectées entre elles, et posséder en plus des points d'accès au réseau public « filaire » si l'on souhaite que les abonnés « mobiles » et « fixes » puissent s'appeler mutuellement. Ce « maillage » du réseau se fait soit par faisceaux hertziens, soit par lignes téléphoniques en cuivre ou en fibres optiques.

Il faut par conséquent bien comprendre que l'utilisation d'un téléphone portable est intégralement tributaire de la présence, de la couverture, du bon fonctionnement, et de la non-saturation, d'au moins un réseau de stations fixes.

Toutes proportions gardées, on pourrait ainsi assimiler les téléphones portables à des « téléphones sans fil » perfectionnés, dont les « bases » seraient non plus privées mais publiques. Cette comparaison se justifie d'autant plus que les nouvelles générations de téléphones sans fil (DECT) s'inspirent assez largement de la technologie GSM…



**Un faisceau hertz
(2 Mb/s, parab
de 30 cm) desserv
une station fi
Au second plan, u
antenne 1 800 M**

Un téléphone portable ne fonctionnera donc pas n'importe où, même si les opérateurs annoncent fièrement des taux de couverture de 95 % et plus (mais au fait, du territoire, ou bien de la population ?). Il doit être tout à fait clair que deux téléphones portables, même en vue directe l'un de l'autre, ne pourront pas communiquer entre eux si un seul de ceux-ci se trouve dans une zone d'ombre du réseau dont il dépend (et cela peut se jouer à quelques mètres près !). Il y a, en effet, aussi peu de points communs que possible entre les téléphones portables, simples « terminaux » tributaires d'un réseau de stations fixes, et les émetteurs-récepteurs autonomes (VHF, BLU, CB, talkie-walkie, etc.). Cette différence fondamentale mérite, on nous pardonnera d'insister, d'être parfaitement assimilée... Or les zones non couvertes, grandes ou petites, ne manquent pas, notamment dans les endroits les moins peuplés, où l'installation de stations fixes ne serait pas suffisamment rentable. On ne pourra même pas, c'est évident, y demander tout simplement du secours en composant le 112.

Oserons-nous écrire que la téléphonie mobile n'a rien d'un « service public » au sens noble du terme, mais tout d'une affaire essentiellement commerciale ?

Une couverture mondiale sans pratiquement aucun « trou » n'est guère possible que par le biais d'un réseau cellulaire dont les stations fixes sont… des satellites.

La beauté technique du système GSM est qu'une communication en cours ne s'interrompt normalement pas lorsque l'on change de cellule (même en roulant à toute vitesse en voiture ou en train), voire même quand on franchit une frontière ! Cela suppose toutefois impérativement, et un homme averti en vaut deux, que le réseau puisse savoir à tout instant où se trouve chaque mobile en état de répondre à un appel…

Il en résulte que tout téléphone portable sous tension (et pas nécessairement en conversation) peut théoriquement être localisé à volonté, avec une précision de quelques centaines de mètres en ville et de quelques kilomètres en rase campagne.

De quoi imaginer, dans un avenir très proche, des services de « troisième génération » basés sur la position géographique (recherche automatisée d'hôtels, restaurants, taxis, etc.).

1.5 UN RÉSEAU INTERNATIONAL

On a vu comment, dès l'origine, le système GSM a été pensé comme un réseau véritablement européen, et par conséquent international.

Depuis le ralliement de très nombreux autres pays, on peut désormais pratiquement parler de réseau mondial.

En principe, cela devrait se traduire, pour tout client de n'importe quel opérateur GSM, par la possibilité d'utiliser son portable au cours de tous ses déplacements dans n'importe quel pays équipé, en restant toujours joignable au travers d'un seul et unique numéro de téléphone.

Dans la pratique, tout dépend de la formule (d'abonnement ou de prépaiement) souscrite auprès de son opérateur domestique, et de ses éventuelles options internationales gratuites ou payantes. Il faut également compter avec les accords passés (ou non !) entre les opérateurs des différents pays, pour échanger leurs services auprès de leurs clients respectifs.

Dans le meilleur des cas, on pourra réellement parcourir le monde tout en continuant à recevoir normalement des appels (mais en payant leur réacheminement), ou des messages écrits (gratuitement), et en conservant la possibilité d'appeler quasiment sans restriction. À défaut, on pourra tout juste atteindre, à l'étranger, les services d'urgence en composant le 112.

En règle générale, les possibilités les plus étendues sont passablement onéreuses, mais nous ferons bientôt découvrir à nos lecteurs comment en bénéficier, sans abonnement, pour à peine plus cher que les formules prépayées de nos opérateurs nationaux...

Le roaming e l'une des possibilit les plus fascinant du GSM

1.6 UN MOBILE BANALISÉ

Dans le domaine de la téléphonie filaire, on sait bien que n'importe quel poste téléphonique (agréé !) peut être branché sur n'importe quelle ligne, dont il adopte instantanément le numéro.

En matière de téléphonie mobile, la notion même de « ligne » n'a aucun sens, et on se doute bien qu'il ne saurait être question qu'un canal radio soit affecté en propre à chaque abonné.

Depuis toujours, un mobile désireux de passer un appel doit commencer par s'identifier auprès du réseau, au moins en vue de la facturation de la communication.

Le moyen d'identification le plus archaïque consiste en un simple indicatif qu'on épelle à une opératrice. Il n'y a encore que peu d'années, les marins procédaient couramment ainsi pour téléphoner à des correspondants à terre... Puis est venue l'automatisation, l'indicatif étant transmis à un système informatique sous la forme d'une succession de tonalités codées.

La déconcertante facilité avec laquelle n'importe qui pouvait usurper l'indicatif d'un abonné pour téléphoner à ses frais, aurait pu suffire à elle seule à stimuler la recherche d'un procédé plus sûr.

Dans le système GSM, le mobile s'identifie toujours auprès du réseau dès sa mise sous tension (puis périodiquement), mais l'opération se fait par un échange crypté de données numériques. Les identifiants et clefs nécessaires résident dans une carte à puce, baptisée SIM (*Subscriber Identification Module*), que l'opérateur confie à son client lors de son adhésion au service.

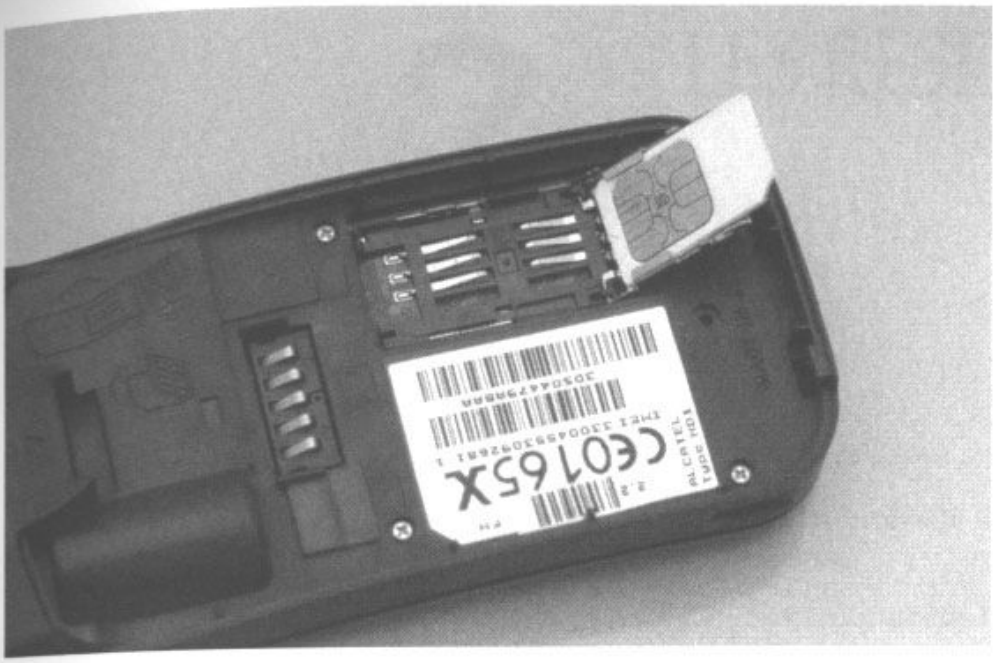
En principe, il suffit de l'insérer dans n'importe quel mobile GSM, pour que celui-ci se trouve aussitôt « branché sur la ligne » du titulaire de la carte SIM : il adoptera son numéro de téléphone, et c'est lui qui paiera les appels émis ou même, dans certains cas, reçus.

L'idée de base est en effet la liberté totale d'utiliser un portable acheté, loué, ou emprunté, lors des circonstances les plus diverses de la vie moderne. Cette idée séduisante d'un téléphone parfaitement « banalisé » se heurte cependant aux dures réalités du monde contemporain :

- La possibilité d'utiliser, en toute simplicité, n'importe quel téléphone volé exciterait bien évidemment la convoitise très au-delà du raisonnable.
- La fourniture de téléphones à des prix anormalement bas, en contrepartie de la souscription d'un abonnement, s'accommoderait mal de la possibilité de succomber du jour au lendemain aux charmes d'un opérateur concurrent.
- Le complet anonymat d'un téléphone portable (si ce n'est de sa carte SIM) serait évidemment insupportable aux autorités policières de bien des pays, même foncièrement attachés au respect de la vie privée et des libertés individuelles…

Chaque téléphone portable actuellement vendu est par conséquent « tatoué » électroniquement avec un numéro d'identification unique (IMEI) qui peut être lu à volonté par le réseau, et éventuellement inscrit sur une « liste noire » tenue par les opérateurs. Il est même bien souvent « verrouillé » sur telle ou telle carte SIM, ou sur tel ou tel opérateur. Cela n'exclut toutefois pas la possibilité d'acheter (mais au prix fort !) des téléphones non verrouillés, ou bien d'obtenir (gratuitement mais laborieusement !) un « code de déverrouillage » au terme d'une certaine durée d'abonnement.

À côté de cela, il n'est pas douteux que des téléphones portables soient couramment déverrouillés, voire débarrassés de leur identifiant compromettant, par d'habiles « pirates » qui dévoilent même parfois leurs « petits secrets » sur Internet…



La carte S
est la vérita
« clef » du GS