OWNI
Digital Journalism

Le 26 janvier 2012
deveryloc
Fabien Soyez

ET VOTRE MOBILE SE CHANGE EN BALISE

Des milliers de localisations cellulaires sont effectuées chaque année en France, notamment dans le cadre de procédures judiciaires. En complément, l'envoi de SMS furtifs est testé. La police collabore principalement avec une entreprise, Deveryware, qui fait le lien avec les opérateurs de téléphonie mobile.

Des SMS furtifs sur vos portables

Les services de sécurité envoient des milliers de SMS furtifs pour localiser des personnes et réactiver leur téléphone ...

En France, le flou domine autour des SMS furtifs. Légalement, rien ne s'oppose à ce que la police française en envoie. Selon le code des postes ou des communications électroniques, les opérateurs doivent effacer ou rendre anonymes les *"données relatives au trafic"*. Seules possibilités de dérogation, celles visant à *"assurer la sécurité du réseau"* ou *"pour les besoins de la poursuite des infractions pénales"*. Les opérateurs peuvent dès lors conserver, pendant un an, les données *"permettant d'identifier l'origine et la localisation de la communication"*.

La police française travaille principalement avec Deveryware, qui collabore avec Orange ou Bouygues. *"L'opérateur de géolocalisation"* propose également Deveryloc, une solution de *"géopointage"* des salariés pour les entreprises, ainsi qu'un service de pistage de vos amis ou de vos enfants, baptisé MyLoc. Deux systèmes de localisation qui se font avec le consentement des personnes suivies. Pour refuser le traçage, la personne pistée peut envoyer un SMS à l'opérateur. Mais dans le cadre d'informations judiciaires, l'avis de la cible n'est pas demandé.

Sur son site, François-Bernard Huyghes, chercheur à l'Institut des Relations Internationales et Stratégiques (IRIS), décrit le système utilisé par Deveryware, appelé localisation cellulaire, ou Cell-id. Un système très vraisemblablement combiné à l'envoi de SMS furtifs, destinés à *"mettre à jour"* l'envoi des signaux d'un mobile :

> L'opérateur fournit en fait une latitude et une longitude approximatives. A tout moment un téléphone mobile est repéré par les trois bornes qui l'entourent et il "choisit" celle sur laquelle la connexion sera la meilleure. Le numéro d'une borne indique donc la zone dans laquelle est la carte SIM. En fait, le système est un peu plus précis, puisque la borne a, en quelque sorte, des "facettes" et que l'on peut savoir vers laquelle est dirigé le téléphone. Parfois, il peut être demandé à l'opérateur d'envoyer secrètement un SMS furtif, c'est-à-dire que l'utilisateur ne recevra jamais et qu'il ne détectera pas, afin de faire « réagir » son téléphone et de mieux le localiser.

Sur son site, Deveryware décrit la façon dont la police utilise ses services :

> Une famille signale aux forces de l'ordre la disparition inquiétante de l'un ses membres. L'officier de police judiciaire traitant le dossier en informe le Procureur de la République. Le magistrat autorise alors l'officier de police judiciaire à réquisitionner l'opérateur GSM et Deveryware pour tenter de localiser la personne disparue. Ainsi, le

Printed with joliprint

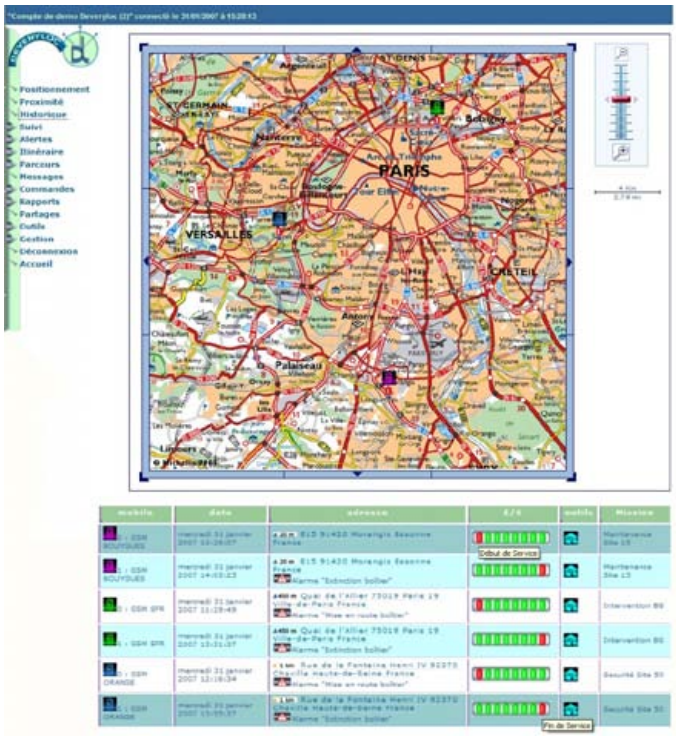
ET VOTRE MOBILE SE CHANGE EN BALISE

Geohub de Deveryware contribue régulièrement à sauver des vies.

Finies les filatures, place au "géopositionnement"

En Juillet 2008, dans Le trait d'union, la revue d'information du syndicat Synergie-Officiers, Jacques Salognon, dirigeant de Deveryware, déclare :

> "Depuis 2003, les opérateurs GSM (Orange puis SFR) ont rendu possible, moyennant rémunération, d'indiquer en temps réel la cellule dans laquelle se trouve un mobile, même s'il est en veille. La localisation cellulaire a déjà aidé à élucider de nombreuses affaires de tous types : bandes organisées, trafics de stupéfiants, enlèvements… et son utilisation par les services déjà initiés progresse régulièrement. Plus de 250 services des forces de l'ordre ont choisi notre solution.



Sébastien Crozier, délégué syndical CFE-CGC-Unsa chez France Télécom-Orange, nous explique qu'à une époque les SMS furtifs étaient la norme :

> "A la base, le SMS n'est pas une fonctionnalité définie pour envoyer des messages, c'est un canal technique réservé à l'opérateur pour pouvoir piloter le téléphone, mettre à jour les paramétrages, sans gêner l'utilisateur, et il est resté technique… On l'a rendu public pour en faire un usage commercial. Mais à la base, les SMS n'avaient pas vocation à être visibles de l'utilisateur.

Historiquement, la localisation cellulaire servait aux appels d'urgence, les bons vieux 15, 17, 18, 115 et 119. Aujourd'hui, "*on l'utilise aussi pour un usage commercial*", affirme Sébastien Crozier. La localisation cellulaire se base sur le protocole RRLP (Radio resource location services protocol). Un protocole dormant, qui permet au réseau d'être en communication permanente avec un mobile, même quand celui-ci est en veille (mais pas éteint).

> "Le réseau passe son temps à scanner, à chercher où se trouve votre mobile. Cela permet au réseau de vous localiser au cas où vous vous apprêtez à passer un appel. Cela permet aussi à certaines boîtes de déclencher l'envoi d'un SMS vers votre mobile lorsque vous passez près d'une boutique de vêtements. Grâce au RRLP, la police peut avoir des informations pour organiser la triangulation. Un SMS furtif permet de réveiller ce protocole.

En 2010, sur 600 000 réquisitions envoyées aux opérateurs téléphoniques par des enquêteurs, 11 000 avaient comme but de géolocaliser une personne. Le reste concernait les traditionnelles mises sur écoute. *"La localisation cellulaire est un grand classique, c'est un mode de localisation standardisé, complètement banalisé"*, indique Sébastien Crozier. En 1999, dans le cadre de l'affaire Colonna, les enquêteurs de la Division natio-

Printed with joliprint

nale anti-terroriste (DNAT), aujourd'hui Sous-direction antiterroriste (SDAT) de la Direction centrale de la police judiciaire (DCPJ), avaient identifié le commando Erignac grâce à la triangulation des téléphones mobiles :

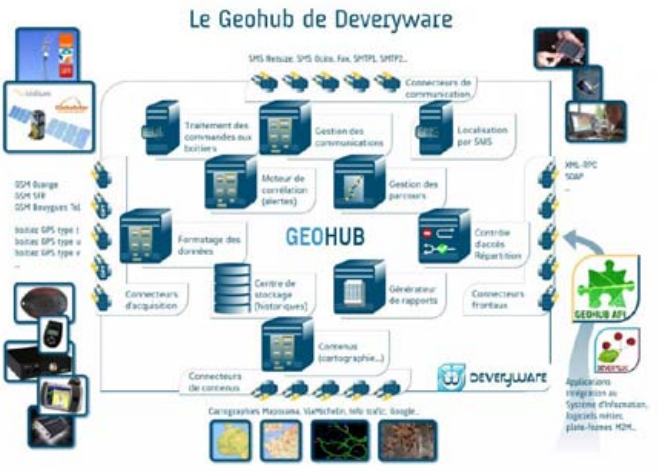
> C'était une forme de localisation primitive, ce n'était pas encore du temps réel. Mais aujourd'hui, on est dans une logique de développement de la data mobile, d'une exploitation commerciale et judiciaire des données. Désormais, si on vous kidnappe et que vous appelez la police depuis le coffre d'une voiture, la police vous retrouvera grâce aux antennes relais.

La police française rame

Laurent Ysern, responsable investigation pour SGP Police, confirme l'expérimentation par la police de la méthode des SMS furtifs pour compléter la localisation cellulaire :

> C'est un système connu et utilisé par les services de renseignement. Mais comme les opérateurs de téléphonie mobile sont propriétaires de leur réseau, l'accès direct aux données est compliqué. Chaque réquisition se fait moyennant finance, et c'est très cher.

Pour la police française, les SMS furtifs sont pour le moment *"difficilement exploitables"* en masse, en raison des *"tarifs élevés"* pratiqués par les opérateurs de téléphonie mobile et de quelques *"bugs"* dûs à des informations livrées *"pas toujours de façon chronologique"*. Comme l'explique Sébastien Crozier, *"le SMS a un inconvénient : sa vocation n'est pas le temps réel, on peut l'utiliser pour mettre à jour la localisation d'un mobile, mais parfois, les serveurs de livraison peuvent planter ou ramer."*



Pas de précisions sur la somme allouée aux opérateurs, mais elle justifie une utilisation *"très limitée"* de la localisation cellulaire et des SMS furtifs. Selon François-Bernard Huyghe, *"un géopositionnement coûte 17 euros par jour à la justice"*, soit environ 500 euros par mois. En 2010, le paiement des frais aux opérateurs électroniques réquisitionnés s'est élevé à 35,6 millions d'euros.

Deveryware fait l'objet de plus d'un millier de réquisitions judiciaires par mois. Et la facture s'avère effectivement salée. Dans un article de Mediapart, on apprend qu'en septembre dernier, le ministère de la Justice, qui paie la note, devait à la société privée quelque 5 millions d'euros. *"La Chancellerie accumule les retards de paiement"*, indique Laurent Ysern à OWNI. En juin 2010, le retard était si important que Deveryware, pour *"assurer sa pérennité"*, avait pris des *"mesures d'économie"* en suspendant leur *"service d'assistance"* durant la nuit et le week-end.

"Il y a une inflation des réquisitions, qui sont de plus en plus complexes, et l'État ne veut pas les payer, du moins à leur juste valeur", constate Sébastien Crozier. Le délégué de la CFE-CGC-Unsa de France-Telecom Orange, qui observe une *"lutte"* entre les opérateurs et la justice pour la rémunération des réquisitions judiciaires.

Printed with joliprint

ET VOTRE MOBILE SE CHANGE EN BALISE

"En France, on est très en retard, suite aux restrictions budgétaires notamment", déplore Laurent Ysern, à SGP Police. Du coup, le ministère de la Justice tente de réduire les coûts : *"les services de police et de renseignement ciblent les affaires les plus importantes"*. La police française se recentre donc sur quelques affaires, et passe en priorité par le Geohub de Deveryware.

Le Graal de la géolocalisation cellulaire

Dans d'autres pays, les services de sécurité sont bien moins frileux. En Allemagne, la police fédérale criminelle (BKA) a envoyé entre 38 000 et 97 000 SMS furtifs par an, entre 2007 et 2011. Dans la même période, le BFV, service de renseignements intérieur, équivalent du FBI en Allemagne, a envoyé pour sa part entre 52 000 et 125 000 "stille SMS" par an. Même les douanes ont utilisé les SMS furtifs, à raison de 227 587 SMS envoyés en six mois.

A Heise online, Mathias Monroy s'inquiète de cet usage immodéré de la localisation cellulaire et des SMS furtifs :

> En février 2011, dans l'État de Saxe, il y a eu une manifestation anti-nazie. La police allemande a tenté d'obtenir les numéros des manifestants en utilisant les antennes relais. Ils sont arrivés à leurs fins, mais beaucoup de personnes, qui ne participaient pas à la manifestation et qui vivaient dans la zone couverte par le réseau GSM surveillé, ont aussi été répertoriées. C'est une méthode utilisée un peu partout, comme en Syrie, ou en Iran.

Aux États-Unis, le FBI utilise un système similaire. Les agents fédéraux dissimulent dans une camionnette une sorte de boitier, le Stingray, qui leur permet de trianguler eux-mêmes les signaux sans passer par les opérateurs. Le Stingray, appartenant à la famille des IMSI Catcher, se fait passer pour une antenne relais, à laquelle la cible va se connecter et envoyer des informations, dont son IMSI, un numéro d'identification unique stocké dans la carte SIM, permettant de l'identifier et de la localiser. Une méthode utilisée par les hackers, reprise façon espionnage. Pour localiser un individu, les agents fédéraux envoient un "ping" au mobile visé, afin de le localiser "tant qu'il reste allumé", indique le Wall Street Journal.

En Grande-Bretagne, entre 2008 et 2010, la Metropolitan Police a acheté une technologie "tenue secrète", mais vraisemblablement un IMSI Catcher, permettant de "se faire passer pour un réseau de téléphonie mobile". Grâce à ce "système clandestin", les policiers peuvent capter les codes IMSI dans des zones ciblées pouvant aller jusqu'à 10 kilomètres carrés, afin de suivre les mouvements de suspects en temps réel, notamment lors de manifestations, comme en 2010 à Londres. Dans le même temps, ils peuvent effectuer des attaques DDOS, afin d'éteindre les mobiles à distance – technique officiellement utilisée pour empêcher le déclenchement d'une bombe via un mobile. Cette technologie a été fournie à la police par la société Datong, qui compte parmi ses clients les services secrets américains, le ministère de la défense britannique et plusieurs régimes du Moyen-Orient.

Concerné par "la protection de la vie privée", le syndicaliste Sébastien Crozier lance :

> On est dans un monde où les données et la liberté privée sont de plus en plus encadrés. Cela pose la question de l'atteinte à la vie privée du citoyen lambda : aujourd'hui, et demain, quels seront les garde-fous qui permettront au citoyen de se protéger ? C'est une question de société qui risque de se poser très prochainement. La question de l'utilisation des données devient un élément clé. On pourrait dire "souriez, vous êtes pistés".

Et de conclure : *"si tout le monde accepte d'être surveillé à longueur de journée, à son insu, on n'est jamais à l'abri des dérives"*.

—

Les illustrations proviennent de Deveryware

Printed with joliprint