

Extrait du Spyworld Actu

<http://www.spyworld-actu.com/spip.php?article10763>

M. Quéméner
(cyber-criminalité) :
"Poursuivre les
cyber-délinquants, protéger
les libertés individuelles, un
dosage savant"



Date de mise en ligne : mercredi 20 mai 2009

- Renseignement - France -

Spyworld Actu

Ce magistrat au service criminel de la Cour d'appel de Versailles dresse un panorama des dispositifs d'écoutes, de veille voire de traques sur les réseaux électroniques. Philippe Guerrier

Dans [l'affaire du "SMS menaçant" qui a éclaté début mai](#), un soupçon d'écoutes électroniques étendus au grand public à l'échelle nationale au nom de la lutte anti-terroriste a plané. Il n'en est rien. Selon le procureur de la république d'Abbeville (Somme), Bouygues Telecom serait hors de cause dans la transmission du SMS à la justice. C'est tout à son honneur puisque tout opérateur est tenu à la confidentialité des messages reçus ou envoyés sur les mobiles de ses clients.

En fait, selon l'AFP, c'est un agent de sécurité de la SNCF qui a transmis les éléments à la justice. En insérant sa carte SIM dans un terminal de prêt, il avait repéré le message SMS "Pour faire dérailler un train, t'as une solution ?" (une plaisanterie au goût douteux). Le supérieur hiérarchique de l'agent de la sécurité avait alors demandé de fournir les informations à la police. La boucle est bouclée.

Néanmoins, les autorités judiciaires disposent de moyens électroniques d'écoutes, d'interception et de veille sophistiqués pour que les enquêtes policières avancent mais ces procédures sont encadrées, assure Myriam Quéméner. Experte dans la lutte anti-cybercriminalité pour le compte du Conseil de l'Europe, elle occupe des fonctions de magistrat au service criminel de la Cour d'appel de Versailles. Pour Vnunet.fr, elle dresse un panorama des dispositifs mis en place (interview réalisée le 5 mai 2009).

Vnunet.fr : Où en est le déploiement de la plate-forme de la délégation aux interceptions judiciaires ?

Myriam Quéméner : Cette plate-forme, rattachée au ministère de la Justice, est opérationnelle depuis deux ans. Les interceptions de communications vocales ou SMS/MMS sont réalisées dans le cadre de réquisitions judiciaires. C'est une requête à destination des opérateurs télécoms ou prestataires techniques. Elle émane soit du Parquet soit du juge d'instruction dans le cas d'une information judiciaire. Le ministère de la Justice a mis en place un référentiel tarifaire sur les réquisitions aux fins d'interceptions sur les réseaux des opérateurs mobiles. Et un projet similaire est en cours d'élaboration pour les réquisitions chez les fournisseurs d'accès Internet. Le projet s'inscrit dans un processus de dématérialisation des réquisitions. Elles seront faites de manière numérique au lieu d'utiliser le fax.

Vnunet.fr : Pouvez-vous préciser le cadre juridique de ces interceptions ?

Myriam Quéméner : Il y a plusieurs cas. Les interceptions peuvent intervenir dans le cadre d'une enquête préliminaire. Sur autorisation du procureur de la république, un officier de police judiciaire (policier ou gendarme) va procéder à cette réquisition prévue par le Code de procédure pénale (article 61). Dans le cadre d'une enquête de flagrance, il faut au préalable une autorisation du juge des libertés et des détentions. Si un juge d'instruction est saisi, c'est lui qui délivre les autorisations de procédures de réquisitions. Cela représente un volume considérable d'interceptions. De l'ordre d'une dizaine de milliers par mois.

Vnunet.fr : Est-ce la seule plate-forme d'écoutes des communications numériques qui existe en France ?

Myriam Quéméner : On trouve également une autre plate-forme de veille exploitée par le Service technique de recherches judiciaires et de documentation (STRJD), basée à Rosny-sous-Bois (Seine-Saint-Denis) et rattachée à

l'Institut de Recherche Criminelle de la Gendarmerie Nationale (IRCGN). Ils ont des moyens renforcés en matière de lutte contre la pédo-pornographie via Internet. Il y a aussi une démarche pro-active sous forme de cyber-patrouilles avec des techniques d'infiltration (ces officiers de police judiciaire habilités peuvent se faire passer pour un mineur sur des salles de discussion en ligne ou tchat). C'était déjà inscrit dans le cadre de la loi sur la Prévention de la délinquance de juin 2007 mais un récent arrêté a précisé le dispositif opérationnel qui se limite à des infractions sur mineurs.

Vnunet.fr : Quelle est la différence de ses plates-formes avec Internet-signalement.gouv.fr ?

Myriam Quéméner : La vocation de cette plate-forme mise en place par le ministère de l'Intérieur est complètement différente : la centralisation des signalements des contenus illicites sur Internet (réception des signalements, traitements et envois aux services judiciaires compétents). Elle est également opérationnelle, même si elle a fait l'objet d'un changement de noms. A l'origine, l'initiative s'appelait Internet-mineurs.gouv.fr. En début d'année, elle a été rebaptisée Internet-signalement.gouv.fr qui a été élargi à toutes les infractions liées aux nouvelles technologies. Le ministère de l'Intérieur l'exploite par l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLTIC) [qui va devenir l'Office central contre la cybercriminalité OCC ou O2C, ndr]. Elle s'est retrouvée sous les phares des médias en début d'année avec [la création d'un groupe dédié aux escroqueries en ligne](#) dans le cadre du projet Pharos.

Vnunet.fr : En conséquence, il n'y aurait pas de risque de surveillance généralisée des écoutes électroniques en France ?

Myriam Quéméner : C'est strictement interdit. L'objectif est de trouver un savant équilibre : poursuivre les cyber-délinquants tout en protégeant les libertés individuelles. La Commission nationale Informatique et Libertés a toujours donné son avis sur ses projets d'interception. Actuellement, un projet de loi Lopsi II (loi d'orientation et de programmation pour la sécurité intérieure) est en cours de discussion. Il y a des dispositions de "captations de données numériques à distance" mais il faut affiner le dispositif de contrôle. Il s'agit d'autoriser des perquisitions à distance via des intrusions dans les systèmes d'information ou de recourir à des logiciels espions et des chevaux de Troie. Ce sont des mesures d'investigation attentatoires à la liberté. On va utiliser des outils de pirate mais ce sera extrêmement contrôlé par un juge. Mais je ne veux pas faire peur aux gens : ces mesures ne s'appliqueront pas dans le cadre de la loi Hadopi par exemple. Uniquement pour des affaires graves comme le terrorisme.

Cyber-criminalité - Défi mondial : la version réactualisée

Myriam Quéméner et Joël Ferry viennent d'éditer la deuxième édition de leur ouvrage Cyber-criminalité - Défi mondial (éditions Economica). Cet ouvrage, qui s'adresse aussi bien aux internautes qu'aux acteurs économiques et aux professionnels du droit, permet d'acquérir une meilleure connaissance de la cyber-criminalité et du dispositif légal de lutte. Son co-auteur Joël Ferry occupe le grade de Colonel de gendarmerie commandant la section de recherches de Versailles. Il a notamment servi à l'Office central de lutte contre la criminalité liée aux technologies de l'information (OCLTIC) et de la communication et à la Direction des affaires criminelles et des grâces.

Post-scriptum :

http://www.vnunet.fr/news/m_quemene...