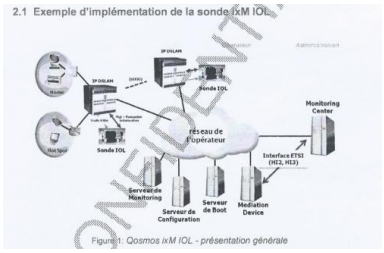
La surveillance du Net a été généralisée dès 2009

PAR JÉRÔME HOURDEAUX
ARTICLE PUBLIÉ LE MERCREDI 8 JUIN 2016



Un schéma expliquant l'installation des sondes dans le réseau ADSL des opérateurs

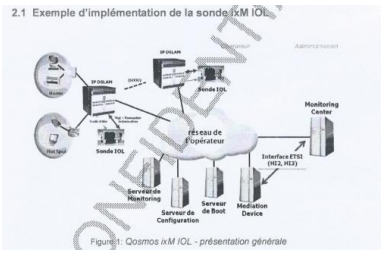
Bien avant les révélations d'Edward Snowden, la France avait mis en place un dispositif de surveillance automatisé de son réseau internet *via* l'installation de sondes sur l'ensemble du réseau ADSL. Ce programme, baptisé « IOL » pour Interceptions obligatoires légales, permettait de collecter *« en temps réel »*les métadonnées, pratique non autorisée à l'époque.

« Moi, assis derrière mon bureau, j'avais certainement l'autorité pour placer sur écoute n'importe qui, vous, votre comptable, un juge fédéral, ou même le président des États-Unis si j'avais un mail personnel. » Ce témoignage, devenu historique, livré par Edward Snowden à Glenn Greenwald en juin 2013 avait provoqué un véritable séisme, symbolisant en une phrase l'étendue des pouvoirs de la NSA, l'agence de sécurité américaine. Il avait suscité, partout dans le monde, des réactions indignées. Ce que l'on sait moins, c'est que le dispositif décrit par le lanceur d'alerte n'était pas si innovant que cela et que d'autres pays, en l'espèce la France, disposaient déjà depuis plusieurs années d'outils similaires dont certains étaient, en théorie, encore interdits.

Certes, les services de renseignement français n'ont jamais disposé des mêmes moyens que leurs homologues américains. Mais plusieurs documents et témoignages recueillis par Mediapart et **Reflets montrent** que le gouvernement a mis en place, à partir de 2009, un dispositif d'écoute de grande ampleur, reposant sur l'installation de « sondes » chez les fournisseurs d'accès à Internet, permettant d'intercepter n'importe quel flux de données de manière automatisée.

Ce programme français, baptisé « IOL » pour « Interceptions obligatoires légales », fonctionnait peu ou prou comme celui décrit par Edward Snowden. À la différence qu'il ne permettait pas exactement de mettre *« n'importe qui »* sur écoute. « IOL » n'était pas un programme clandestin, mais s'inscrivait dans le cadre de la procédure d'autorisation des écoutes administratives. Ses cibles, après avoir été déterminées par les services demandeurs, étaient ensuite transmises pour validation au Groupement interministériel de contrôle (GIC), organe dépendant du premier ministre et chargé de mettre en œuvre les écoutes.

Mais techniquement, les services français n'avaient pas à rougir de leurs collègues américains. Concrètement, IOL reposait sur l'installation de « sondes » sur le réseau, plus précisément sur les « DSLAM », des boîtiers permettant de relier un groupe de lignes téléphoniques au réseau internet en ADSL. Ces sondes effectuent en permanence une *« analyse du trafic »*, assurant ainsi une surveillance passive du réseau. Lorsqu'une cible était validée par le GIC, il suffisait d'entrer dans un logiciel un identifiant lui correspondant. Dès que celui-ci était repéré dans le flux, la sonde déterminait l'adresse IP, permettant de localiser le lieu de connexion et de détourner le trafic associé vers un « *monitoring center* ».



Un schéma expliquant l'installation des sondes dans le réseau ADSL des opérateurs

Un projet de guide de configuration de ces sondes, datant de 2009, alors que le dispositif était en cours de développement, que Mediapart et Reflets ont pu consulter, résume leur fonctionnement. *« L'interception est fondée sur une liste contenant les identifiants des cibles. L'application détermine l'adresse IP d'une cible, dont l'un au moins des*

identifiants a été reconnu dans le trafic analysé par la sonde », explique la société Qosmos qui a développé ce système. Une fois la cible repérée dans le flux de communications, *« les sondes IOL remontent le trafic intercepté (…) vers un Mediation Device qui le convertit (…) avant l'envoi au Monitoring Center »*.

Si la procédure respecte la loi concernant les écoutes, le dispositif technique d'IOL est juridiquement beaucoup plus problématique qu'il n'y paraît. En effet, les sondes installées par les fournisseurs d'accès fonctionnaient en analysant *« en temps réel »* le trafic et donc les *« données de connexion »* ou métadonnées, c'est-à-dire les données entourant un paquet d'informations. Pour un mail, par exemple, ces métadonnées seront par exemple les identifiants de l'expéditeur et du récepteur, la date et l'heure de l'envoi, la longueur du message…

Ces dernières années, l'analyse de ces métadonnées est devenue une priorité pour les services qui espèrent, grâce à l'application d'algorithmes, détecter dans la masse de métadonnées les *« signaux faibles »*, c'est-à-dire les traces laissées en ligne par leurs cibles. En résumé, plutôt que de miser sur le renseignement humain, les services espèrent détecter les terroristes en analysant de manière automatique leurs interactions en ligne, leurs visites de sites, échanges de mails…

Or, au moment de l'installation du dispositif IOL, la collecte en temps réel de ces données de connexion était strictement interdite. Le régime alors en vigueur avait été fixé par la loi antiterroriste du 23 janvier 2006. Celle-ci permettait la consultation des métadonnées mais *a posteriori*, chez les opérateurs qui avaient l'obligation de les conserver durant une année. L'analyse *« en temps réel »* des métadonnées et sur *« sollicitation du réseau »* n'a officiellement été autorisée que par l'article 20 de la loi de programmation militaire votée en décembre 2013 et dont le décret d'application n'a été publié qu'un an plus tard, le 26 décembre 2014. Ce n'est donc qu'à compter du 1er janvier 2015 que les services ont eu le droit de piocher immédiatement dans les métadonnées.

Des pratiques "a-légales"

Que faisaient les services de ces métadonnées ? Étaient-elles traitées ? Par qui et sur quel fondement juridique ? Contactés, ni le cabinet du premier ministre, ni la société Qosmos ou les opérateurs concernés n'ont répondu à nos questions. Un ancien haut cadre d'un fournisseur d'accès nous confirme pourtant que les métadonnées étaient bien collectées *« en temps réel, à distance »*. C'était d'ailleurs *« tout l'intérêt de cet outil par rapport aux dispositifs historiques pour l'interception de données qui reposaient sur des sondes avec stockage temporaire »*, précise-t-il.

Au niveau juridique, un contournement de la loi n'aurait rien de surprenant : le contrôle des interceptions de métadonnées était, en 2009, particulièrement léger. La loi du 23 janvier 2006 avait en effet confié leur autorisation à une *« personne qualifiée »* dépendant du ministre de l'intérieur, le contrôle de la Commission nationale de contrôle des interceptions de sécurité (CNCIS) n'intervenant qu'*a posteriori*.

Au mois de novembre 2014, le président de la CNCIS, Jean-Marie Delarue, s'était par ailleurs lui-même alarmé devant des députés du manque de contrôle des interceptions de métadonnées. Regrettant que ce contrôle ne s'exerce qu'après coup, il s'interrogeait également sur *« l'indépendance »* d'une *« personne qualifiée »* dépendant du ministère de l'intérieur qui, lui-même, fait partie des demandeurs d'interceptions.

Ces inquiétudes étaient d'autant plus fondées que les années 2008-2009-2010 semblent avoir été une période d'intenses activités pour les opérations « a-légales » des services. En septembre 2010, *Le Canard enchaîné* puis *Le Monde* avaient par exemple révélé que Jean-Paul Faugère, directeur de cabinet du premier ministre d'alors, François Fillon, avait signé un courrier classé *« confidentiel défense »***autorisant les services à se procurer les *« données techniques »* téléphoniques**, c'est-à-dire les « fadettes », directement chez les opérateurs, en passant outre le contrôle de la CNCIS.

De son côté, au mois de juillet 2015, *L'Obs* avait révélé l'existence **d'un décret secret signé en 2008** autorisant la DGSE, le renseignement extérieur, à se brancher directement sur les câbles transatlantiques afin d'espionner les communications internationales.

Concernant le dispositif IOL, ses sondes avaient été déployées chez les principaux fournisseurs d'accès à Internet, *« soit près de 99 % du trafic résidentiel »*, nous indique une source interne. Chaque opérateur avait la liberté, dans le cadre de la convention passée avec le GIC, de choisir son propre prestataire. Mais une partie de ce marché a été emportée par le leader du secteur, la société Qosmos à qui Mediapart et Reflets ont déjà consacré plusieurs enquêtes.

Qosmos est notamment connue pour être visée par une information judiciaire pour complicité d'actes de torture en Syrie. La justice reproche à la société d'avoir participé à la vente d'un système d'espionnage à Bachar al-Assad et essaye de déterminer si ses sondes ont bien été opérationnelles et ont permis l'arrestation d'opposants torturés. Dans le cadre de cette procédure, la société a été placée sous le statut de témoin assisté au mois d'avril dernier.

Le produit phare de Qosmos, celui vendu à la Syrie, est le ixM-LI (pour Legal Interception). Et c'est également celui fourni dans le cadre du projet IOL. Selon nos informations, le dispositif IOL a commencé à être imaginé dès 2005, avec la rédaction d'un cahier des charges en 2006, des tests en 2007 et enfin un déploiement au cours de l'année 2009. Des documents internes de Qosmos que Mediapart et Reflets ont pu consulter montrent que, en 2012, la société livrait un « patch », c'est-à-dire un correctif ou une mise à jour, pour la version « 2.1.3 » de la sonde « ixM-IOL ».

Par ailleurs, toujours en 2012, les policiers travaillant sur l'affaire de la vente de sondes au régime de Bachar al-Assad avaient tenté d'obtenir la liste des clients de Qosmos. Quatre d'entre eux étaient classés *« confidentiel défense »* et désignés uniquement sous des noms de code. L'un d'eux était « IOL ». L'ancien haut cadre d'un opérateur nous confirme que le programme était bien encore actif en 2013-2014. En revanche, le dispositif a de fortes chances d'être ensuite devenu obsolète, tout d'abord pour des raisons techniques liées à l'évolution du réseau internet. Ensuite en raison du vote de la loi sur le renseignement, instituant le dispositif des boîtes noires.

La révélation de l'existence de ce programme confirme en tout cas deux choses. Tout d'abord, comme l'a revendiqué le gouvernement lui-même, les différentes lois sécuritaires votées ces dernières années (LPM, loi sur le renseignement, loi sur les communications internationales…) ne faisaient que donner un cadre légal à des techniques qualifiées par l'euphémisme « a-légales », mais en réalité non autorisées par la loi.

Ensuite, les autorités n'hésitent pas à pratiquer, dans ce domaine, le double langage. Alors que **les liens entre les autorités françaises et des sociétés telles que Qosmos** ont été à plusieurs reprises révélés par la presse, que ce soit à travers le projet IOL ou le projet Kairos, ces programmes n'ont jamais été évoqués, ne serait-ce que dans leurs grandes lignes, lors des débats parlementaires.

Une anecdote, relayée par Reflets au mois de novembre 2014, est symbolique de ce jeu de dupes. Le président de la commission des lois, président de la délégation parlementaire du renseignement, futur artisan de la loi sur le renseignement et désormais ministre de la justice, Jean-Jacques Urvoas, avait été auditionné par la Commission parlementaire sur les libertés à l'âge du numérique à laquelle participait le directeur de Mediapart, Edwy Plenel. Ce dernier avait interrogé le député sur les liens entre l'État et la société Qosmos après la publication d'une première enquête sur ce sujet. *« Je n'ai jamais rencontré, depuis que je suis (…) président de la délégation parlementaire au renseignement, cette structure, je n'ai jamais entendu qu'elle soit un prestataire de qui que ce soit, en tout cas pas pour les organes qu'il m'arrive de fréquenter »*, **avait répondu Jean-Jacques Urvoas**.

Directeur de la publication : Edwy Plenel
Directeur éditorial : François Bonnet
Le journal MEDIAPART est édité par la Société Editrice de Mediapart (SAS).
Durée de la société : quatre-vingt-dix-neuf ans à compter du 24 octobre 2007.
Capital social : 28 501,20€.
Immatriculée sous le numéro 500 631 932 RCS PARIS. Numéro de Commission paritaire des publications et agences de presse : 1214Y90071 et 1219Y90071.
Conseil d'administration : François Bonnet, Michel Broué, Gérard Cicurel, Laurent Mauduit, Edwy Plenel (Président), Marie-Hélène Smiéjan, Thierry Wilhelm. Actionnaires directs et indirects : Godefroy Beauvallet, François Bonnet, Laurent Mauduit, Edwy Plenel, Marie-Hélène Smiéjan ; Laurent Chemla, F. Vitrani ; Société Ecofinance, Société Doxa, Société des Amis de Mediapart.
Rédaction et administration : 8 passage Brulon 75012 Paris
Courriel : contact@mediapart.fr
Téléphone : + 33 (0) 1 44 68 99 08
Télécopie : + 33 (0) 1 44 68 01 90
Propriétaire, éditeur, imprimeur : la Société Editrice de Mediapart, Société par actions simplifiée au capital de 28 501,20€, immatriculée sous le numéro 500 631 932 RCS PARIS, dont le siège social est situé au 8 passage Brulon, 75012 Paris.
Abonnement : pour toute information, question ou conseil, le service abonné de Mediapart peut être contacté par courriel à l'adresse : serviceabonnement@mediapart.fr. ou par courrier à l'adresse : Service abonnés Mediapart, 4, rue Saint Hilaire 86000 Poitiers. Vous pouvez également adresser vos courriers à Société Editrice de Mediapart, 8 passage Brulon, 75012 Paris.