# Surveillance : les boîtes noires de Qosmos étaient restées dans l'ombre

Officialisées par la loi sur le renseignement votée en juin dernier, les boîtes noires, ces appareils renfermant des algorithmes de détection de comportements en ligne jugés suspects installés sur les réseaux des opérateurs, FAI et hébergeurs, ont, en réalité, vécu des années dans l'ombre. Selon nos confrères de *Mediapart* et de *Reflets.info*, des boîtiers d'interception conçus par la société française Qosmos étaient présents chez tous les grands opérateurs depuis 2009. Le projet aurait même été sur la table dès 2005, avec une rédaction du cahier des charges finalisée l'année suivante.

Ces boîtes noires, auxquelles les opérateurs n'avaient pas accès, étaient exploitées dans le cadre d'écoutes administratives, commandées par le Premier ministre. Le contrat, connu sous le nom de code IOL (pour Interceptions Obligations Légales) chez Qosmos, prévoyait de couvrir pas moins de 6 000 DSLAM (le multiplexeur permettant d'amener l'ADSL sur le réseau cuivre). Selon *Reflets.info*, en tenant compte du fait que chacun de ces équipements permettait à l'époque d'accueillir entre 384 et 1008 lignes ADSL, ce sont entre 2,3 et 6 millions d'abonnés qui étaient ainsi potentiellement écoutés.

## Des boîtes noires dans le brouillard

Toutefois, chez un opérateur, un responsable interrogé par *Reflets.info* tempère l'intérêt réel du dispositif pour des interceptions en temps réel sur de grands volumes de données. Pour trois raisons selon lui : la part du trafic chiffré, l'évolution des infrastructures et les différences qui existent entre un démonstrateur et un déploiement dans des environnements de production. Façon de dire que les boîtiers Qosmos fonctionnaient mieux en labo qu'en production…

A cette époque, notons également que les technologies d'analyse en temps réel ne permettaient probablement pas de réaliser simplement des traitements sur des volumes aussi massifs. Les documents de Qosmos précisent tout de même que le système était en mesure d'analyser 80 000 paquets IP à la seconde. Et que IOL pouvait définir comme cible des plages entières d'adresses IP. Malgré ces caractéristiques techniques, le dispositif semblait devoir trouver son efficacité maximale sur des cibles pré-définies.

Mais il n'en reste pas moins que IOL masquait bien un système d'interception temps réel des données et métadonnées du trafic Internet des Français. Un exercice qui n'a été officiellement autorisé qu'à posteriori, via le vote de la Loi de programmation militaire de 2013 et un décret publié fin 2014.

Qosmos indique s'être retiré du marché de l'interception légale en 2012. Pour *Reflets.info*, un doute subsiste sur l'évolution de l'infrastructure IOL après cette date.

**A lire aussi :**

Renseignement : le Sénat adopte les boîtes noires, les hébergeurs dans l'expectative

Renseignement : pour l’Inria, les boîtes noires seront inefficaces

**crédit photo © kurhan- shutterstock**