Renseignement : derrière le brouillard juridique, la légalisation du Deep Packet Inspection

Félix Tréguer

Renseignement : derrière le brouillard juridique, la légalisation du Deep Packet Inspection

Félix Tréguer

15 novembre 2017

La Quadrature du Net

URL : https://www.laquadrature.net/fr/renseignement_l%C3%A9galisation_dpi

---

Ça y est, les boîtes noires sont activées !

Après avoir fait couler beaucoup d'encre en 2015 lors de l'adoption de la loi renseignement, ces sondes dédiées à la surveillance en temps réel des communications Internet de millions de résidents français sont désormais employées légalement par les services dans le but de repérer certaines communications « suspectes ». C'est ce qu'a annoncé Francis Delon, le président de la Commission nationale de contrôle des techniques de renseignement (CNCTR) lors d'un colloque mardi 14 novembre à Grenoble.

Sauf que cette annonce est l'arbre qui cache la forêt. On nous explique que le « contenu » des communications n'est pas concerné, et que le secret des correspondances est donc sauf. Mais lorsqu'on lit entre les lignes de la loi et que l'on suit les quelques journalistes d'investigation qui planchent sur le sujet, il est clair que **le droit français cherche depuis 2013 à légaliser l'usage des techniques de « Deep Packet Inspection »**, lesquelles constituent en fait le point d'articulation entre différentes logiques du renseignement technique contemporain.

Jusqu'à présent, chez les défenseurs des libertés publiques intéressés par le renseignement – militants, juristes, universitaires, etc. –, nous étions nombreux à suspecter le recours à de telles techniques de surveillance sans comprendre précisément comment elles pouvaient s'inscrire dans le cadre juridique. En réalité, certaines ambiguïtés légistiques faisaient obstacle à la compréhension de l'articulation droit/technique, faute de transparence sur la nature des outils techniques utilisés par les services et leurs usages.

Or, compte tenu des informations révélées par Reflets.info et Mediapart l'an dernier sur des sondes DPI installées dès 2009 chez les grands fournisseurs d'accès français, **on peut raisonnablement penser que les « boîtes noires » sont en réalité déjà expérimentées depuis longtemps**.

Certes, l'efficacité opérationnelle de tels outils reste à démontrer, compte tenu notamment de l'augmentation du trafic Internet chiffré ces dernières années. Mais depuis 2013, et plus encore depuis 2016, le droit français autorise ces sondes à scanner le trafic d'une grande part de la

population pour « flasher » depuis les réseaux des opérateurs télécoms français certains « sélecteurs » : il peut s'agir de données de connexion traitées par les FAI (notamment l'IP d'origine, l'IP de destination), mais aussi toutes sortes de métadonnées décelables dans ce trafic et traitées par les serveurs consultés, notamment les « protocoles » associés à certains services en ligne et des identifiants non chiffrés (pseudos, hash de mots de passe, etc.). À travers cette analyse du trafic Internet, les services peuvent repérer des cibles, voire même dresser des graphes sociaux détaillés (qui communique avec qui, quand, à l'aide de quel service en ligne, etc.).

Le mécanisme juridique qui permet ces formes de surveillance sur le territoire repose sur **l'exploitation stratégique par les services de renseignement de la distinction entre métadonnées et contenu des communications** : au lieu de considérer les identifiants associés aux services en ligne comme le contenu des communications acheminées par les FAI – ce qu'ils sont au plan technique –, ces identifiants contenus dans les paquets conservent le statut juridique de métadonnées, et peuvent ainsi être collectés à l'aide d'outils DPI.

Inaugurée en 2013 par la LPM (Loi de programmation militaire) et reconduite par la loi renseignement pour la lutte antiterroriste, cette surveillance en temps réel des identifiants contenus dans les communications Internet permet aux services de massifier la surveillance, en contournant les quotas prévus en matière d'interceptions de sécurité (plafond de 2000 interceptions simultanées, pour cette technique qui permet de collecter les métadonnées et le contenu des messages).

Ce texte revient sur cette construction juridique en lien avec l'évolution des techniques de renseignement, et tente d'illustrer la manière dont elle permet de combiner une surveillance automatisée et exploratoire à travers des outils *Big Data* et des interceptions « ciblées » de l'ensemble du trafic de cibles précisément identifiées. Mais avant d'entrer dans le vif du sujet, revenons sur certains éléments de contexte.

1. Éléments de contexte

1.1 Le renseignement et l'exploitation des failles juridiques

D'abord, il faut bien avoir en tête que **les services sauront s’immiscer dans n'importe quelle petite faille juridique** pour trouver une assise juridique à des outils techniques et des pratiques policières très contestables, mais sur lesquelles – faute d'un Snowden à la française (et malgré certaines enquêtes journalistiques qui ont fait sensation) – même les gens qui suivent le sujet d'assez près se heurtent au secret d'État.

On a donc tendance à se rendre compte bien tard de ces failles juridiques et de la manière dont elles sont exploitées au plan opérationnel, et on se demande alors comment on a pu passer à côté tout ce temps-là. Cette mauvaise articulation des raisonnements entre droit et outils techniques contribue à ce que les droits fondamentaux aient toujours plusieurs trains de retard sur les pratiques de surveillance.

Il y a plein d'exemples de ce que je décris ici, comme la surveillance hertzienne inaugurée en 1991. Je vais en détailler un autre, parce qu'il est essentiel à la démonstration, et il est central pour les enjeux contemporains de la surveillance en France. Il concerne l'accès administratif aux informations et documents détenus par les opérateurs télécoms et hébergeurs.

1.2 L'exemple de l'accès aux métadonnées

Pour rappel, l'obligation de conservation des données de connexion (souvent synonyme d'un autre terme bien plus vague sur lequel on va revenir, celui d'« informations et documents » détenus par les intermédiaires technique) date au plan législatif de 2001 pour les opérateurs, de 2004 pour les fournisseurs de services en ligne (c'est-à-dire des personnes physiques ou morales qui mettent à disposition du public des services de communication au public en ligne et stockent des données : hébergeur, réseau social, forum, site de eCommerce, fournisseur public de messagerie, etc.).

Rappelons aussi quelques unes des données concernées par ces obligations de conservation – c'est important pour la suite.

Pour les opérateurs télécoms et FAI :

- les informations permettant d'identifier l'utilisateur (les noms, prénoms et adresse données par l'abonné à son FAI) ;
- les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication (quelle adresse IP était donnée à qui, à quelle date pendant combien de temps) ;
- les données relatives aux équipements terminaux de communication utilisés (adresse MAC, des données relatives à des cookies ou autres identifiants de session détenus par le FAI) ;
- les données permettant d'identifier le ou les destinataires de la communication (*a priori* pour Internet, l'IP de destination, mais on a des doutes sur le fait que techniquement les FAI acceptent de stocker tout ça, car toutes les IP consultées par toute la population française, ça fait beaucoup de données et donc ça coûte cher à conserver. Bref, on est pas sûr – et en soit cette incertitude est déjà révélatrice d'un vrai problème –, mais on peut faire l'hypothèse que les FAI ne les conservent pas, en tout cas pas par défaut).

Pour les hébergeurs / fournisseurs de service en ligne :

- l'identifiant de la connexion à l'origine de la communication (on comprend que c'est ce qu'on appelle vulgairement le *log in* : ça peut être l'alias Twitter, l'adresse mail pour se connecter à sa messagerie, son identifiant Facebook, etc.) ;
- les types de protocoles utilisés pour la connexion au service (Gmail, Facebook, Telegram, Tor et quantité d'autres services en ligne ont des protocoles spécifiques qui sont en quelque sorte leurs signatures) ;
- le mot de passe (*a priori* hashé, dans un format qui ne permet pas de retrouver le mot de passe, mais au moins de vérifier sa signature, son empreinte).

L'accès à ces données de connexion a été ouvert aux services en 2006 pour la seule lutte antiterroriste et pour les seuls opérateurs télécoms. Des techniciens au fait de ces histoires nous expliquaient que les opérateurs ne conservaient pas les IP consultées. Cet accès aux données de connexion était donc uniquement censé permettre d'identifier des suspects de terrorisme dont on aurait récupéré l'adresse IP, en demandant au FAI les noms et prénoms correspondant à cette IP. Pas si choquant me direz-vous. C'est vrai, surtout en comparaison des choses révélées ces dernières années, notamment par Snowden.

Mais dans un rapport de l'Assemblée nationale publié en mai 2013, soit juste avant le début des révélations Snowden, il était écrit que **pour contourner cette restriction du décret de 2006 et accéder aux métadonnées pour d'autres motifs que l'antiterrorisme, les services s'appuyaient sur une disposition, l'article L. 244-2 du code de la sécurité intérieure**, créé en 1991.1

1.3 La LPM : blanchiment législatif de l'illégal

C'est précisément ce **détournement que la LPM a permis de légaliser**, quelques mois plus tard, en élargissant drastiquement la manière dont les services pouvait accéder à ces données : non plus pour la seule lutte antiterroriste, mais pour l'ensemble de leurs missions. Première rupture juridique.

Citons la loi, c'est important :

> Pour les finalités énumérées à l'article L. 241-2, peut être autorisé le recueil, auprès des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications [cet article a été repris par la loi renseignement et est aujourd'hui à l'article L. 851-1 du CSI.

À quoi renvoie ce terme d'« informations et documents » ? On s'en est beaucoup inquiétés à l'époque de l'examen de la LPM, car nous trouvions l'expression extrêmement vague. Mais le gouvernement et les parlementaires qui soutenaient le texte tentaient de nous rassurer en disant qu'il s'agissait un vocable ancien, datant de la loi de 1991, qu'il renvoyait simplement aux métadonnées, et non pas aux informations ou documents contenus dans les messages.

Résumons donc cette deuxième rupture juridique : **les services peuvent désormais accéder non plus aux données des seuls opérateurs télécoms, mais aux « informations et documents » non seulement conservés mais également « traités » par les opérateurs télécoms ou fournisseurs de service**, notamment des données relatives aux « identifiants de connexion » (des log-in, typiquement) ou à la géolocalisation des terminaux.

Ces données sont donc « recueillies » sur demande des services, notamment *via* ce qui constitue la troisième rupture juridique introduite par la LPM : il ne s'agit plus seulement d'accéder *a posteriori* aux données conservées par les intermédiaires techniques (FAI et hébergeurs donc), mais également **« en temps réel » sur « sollicitation du réseau »** :

> Art. L. 246-3.-Pour les finalités énumérées à l'article L. 241-2, les informations ou documents mentionnés à l'article L. 246-1 peuvent être recueillis sur sollicitation du réseau et transmis en temps réel par les opérateurs aux agents mentionnés au I de l'article L. 246-2 ».

Là encore, cela nous avait beaucoup inquiété, sans qu'on réussisse bien à comprendre ce qui se jouait là.

Un an plus tard, en catimini le 24 décembre 2014, le gouvernement fait paraître le décret d'application. Ouf ! Les « informations et documents » sont bien limités aux métadonnées, leur définition n'est pas élargie par rapport aux décrets de 2006 et 2011, comme la loi pouvait pourtant y inviter. En effet, le décret précise (R. 241-1 CSI) :

> Pour l'application de l'article L. 246-1, les informations et les documents pouvant faire, à l'exclusion de tout autre, l'objet d'une demande de recueil sont ceux énumérés aux articles R. 1013 et R. 10-14 du code des postes et des communications électroniques et à l'article 1 er du décret n° 2011-219 du 25 février 2011 modifié relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.

Une autre disposition précise qu'il peut s'agir aussi de données de gélolocalisation des terminaux. Quant à la notion de « sollicitation en temps réel » du réseau, là encore, la CNIL – consultée pour avis sur le décret, se dit satisfaite. Marc Rees écrit à l'époque :

> Le décret prévoit ici que cette sollicitation « *est effectuée par l'opérateur qui exploite le réseau* », et non pas par les autorités elles-mêmes. La CNIL estime dès lors que cette formulation « *interdit toute possibilité d'aspiration massive et directe des données par les services concernés et, plus généralement, tout accès direct des agents des services de renseignement aux réseaux des opérateurs, dans la mesure où l'intervention sur les réseaux concernés est réalisée par les opérateurs de communication eux-mêmes.* »

À ce moment-là, les opposants à la LPM sont en quelque sorte rassurés – le décret pose plein de problèmes, mais la surveillance massive semble désormais impossible.

1.4 Le coup de toilette de la loi renseignement

Six mois plus tard, la version promulguée en juillet 2015 de **la loi renseignement reprend le vocable de la LPM mais réorganise l'accès aux métadonnées** comme suit :

- L 851-1 : accès *a posteriori* aux métadonnées conservées par les FAI et hébergeurs et aux données de gélolocalisation ;
- L 851-2 : accès en temps réel aux métadonnées des FAI et hébergeurs pour les personnes « susceptibles d'être en lien avec une menace » terroriste (alors que dans la LPM, c'était pour l'ensemble des finalités) ;
- L 851-3 : boîtes noires : aka traitements automatisés des métadonnées, conservées par les FAI ou hébergeurs, pour repérer des communications suspectes en lien avec le terrorisme ;
- L 851-4 : géolocalisation en temps réel des terminaux.

À bien des égards, **la loi renseignement apporte des garanties supplémentaires par rapport à la LPM** : « normalisation » des procédures de contrôle préalables sous l'égide de la CNCTR pour l'accès aux métadonnées (plus simplement une personnalité qualifiée qui autorise), restriction de l'accès en temps réel et des boîtes noires à la seule lutte antiterroriste. Comme si les responsables des services avaient eu peur de ce que la loi les autorisait à faire… Ou comme si certains au sein de l'État avaient voulu remettre un peu de mesure dans l'utilisation de dispositifs de surveillance extrêmement intrusifs.

2. De la difficulté de comprendre comment le droit marche en pratique

Depuis le vote de la loi renseignement, les Exégètes amateurs (groupe d'action contentieuse commun aux associations La Quadrature du Net, FDN et Fédération FDN) ont déposé plusieurs recours devant le Conseil d'État qui touchent à l'ensemble de la loi.

Après une QPC remportée sur la question de la surveillance hertzienne en octobre 2016, le Conseil constitutionnel nous a donné gain de cause sur un autre recours relatif à l'accès en temps réel aux données de connexion. La disposition avait déjà été validée dans la décision du Conseil sur la loi renseignement en juillet 2015, mais un an plus tard, après les attentats de Nice, elle a été élargie non seulement aux personnes susceptibles d'être en lien avec une menace, mais à leur entourage, et aux personnes en lien avec cet entourage (les « n + 2 »). Les n+2 de 11 000 fichés S, ça fait potentiellement des centaines de milliers de personnes. Beaucoup de monde donc.

2.1 L'exemple de la QPC sur la surveillance en temps réel

Ce à quoi nous nous heurtions dans nos raisonnements dans ce dossier, c'est la manière dont le droit est mis en musique au plan opérationnel. Par exemple, on comprenait bien l'intérêt pour la surveillance en temps réel des métadonnées téléphoniques, et en soi, c'est déjà extrêmement intrusif. En gros, la loi donne accès en temps réel au journal d'appel détaillé des personnes visées. Plutôt que de s'embêter à faire une interception ciblée, on recueille en temps réel les métadonnées et on fait le graphe social de la personne – qui elle appelle, qui l'appelle, à quelle heure, combien de temps –, le tout étant automatisé grâce à des outils *Big Data*. Cela nécessite moins de ressources que d'éplucher le détail des conversations téléphoniques, et c'est donc d'une certaine manière plus efficace.

Mais pour Internet, on était moins sûr. On réfléchissait généralement de cette manière (un raisonnement analogue vaudrait pour les boîtes noires du L. 851-3 CSI) :

- **côté FAI** : les outils de surveillance qui font la sollicitation sont installées sur des bouts de réseau, et interceptent les métadonnées des FAI (et seulement des FAI) : IP d'origine, et peut être IP consultées (mais comme on raisonne à partir des données « conservées », et qu'on ne pense pas que les IP consultées soient conservées par les FAI, on avait en quelque sorte des œillères qui nous faisait penser que ça pouvait ne pas être le cas – on passait à côté du mot « traitées »). Et puis une IP consultée, c'est intéressant mais relativement aléatoire : il peut y avoir derrière une même IP de nombreux services en ligne différents ; ça ne permet pas d'avoir une granularité très fine de qui communique avec qui.
- **côté hébergeur** : dans ce cas, on s'imagine que les outils de surveillance sont installés sur les serveurs pour scanner les communication et repérer les métadonnées. Ici, les métadonnées (protocoles, identifiants, mots de passe, etc.) sont beaucoup plus fines, et donc intéressantes. Mais il y a un problème pratique. Pour des petits hébergeurs, l'intérêt est limité : on voit passer peu de trafic en réalité, il faudrait faire de la surveillance sur des milliers de serveurs pour avoir une masse critique de trafic dans laquelle piocher des choses intéressantes. Pour les gros, genre Google, Facebook, Twitter, c'est évidemment plus intéressant mais ce sont des entreprises américaines, ce qui pose un problème stratégique (risque que les activités de surveillance des services français ne soient accessibles aux

agences américaines, par exemple). Cela pose aussi un problème plus politique, car on les voit mal, dans le contexte post-Snowden où ces entreprises cherchent à regagner la confiance des utilisateurs, les voir accepter – même sous la contrainte du droit français – avec les services pour installer des boîtes noires ou faire de la surveillance en temps réel (même si c'est par exemple ce que Yahoo est accusé d'avoir fait pour le compte de la NSA).

S'agissant des boîtes noires, le ministre Jean-Yves Le Drian avait par exemple indiqué lors de l'examen parlementaire de la loi renseignement qu'il s'agissait de repérer des communications suspectes. Bertrand Bajolet, qui a quitté il y a quelques mois la direction générale de la DGSE, avait été plus disert à l'époque: « Il s'agit de détecter certaines pratiques de communication. L'objectif n'est pas de surveiller des comportements sociaux, tels que la fréquentation de telle ou telle mosquée par telle ou telle personne. Mais nous connaissons les techniques qu'emploient les djihadistes pour dissimuler leurs communications et échapper à toute surveillance : ce sont ces attitudes de clandestinité qu'il s'agit de détecter afin de prévenir des attentats (…). »

Sur les attitudes de clandestinité, l'allusion évoque assez directement l'utilisation de solution de chiffrement. Au hasard l'utilisation du réseau Tor.

Mais ce qu'on ne comprenait pas, c'est comment les boîtes noires installées sur les réseaux des FAI pouvaient permettre de déceler ce type de comportements. Il nous semblait que les seules choses que la loi autorisait de faire, c'était de flasher les données de connexion du FAI : l'IP d'origine et éventuellement l'IP consultée, l'adresse MAC, ainsi que d'autres infos dans l'entête des paquets.

On comprenait d'autant moins que dans la jurisprudence constitutionnelle du 24 juillet 2015, suscitée par le tout premier recours des Exégètes, le Conseil constitutionnel avait limité le champ de la notion d'« information et documents » aux articles déjà existants issus des décrets de 2006 et de 2011. Une décision qui semblait aller dans notre sens. Elle rappelle notamment que les données de connexion concernées ne peuvent en aucun cas « porter sur le contenu de correspondances ou les informations consultées », ce qui du point de vue des opérateurs télécoms semble de nature à exclure le DPI.

Et puis dans le même temps, le ministre de l'Intérieur d'alors, un certain Bernard Cazeneuve, nous jurait qu'il était « hors de question » d'utiliser du DPI. Il faut croire qu'on a eu envie de lui laisser le bénéfice du doute.

2.2 Ce qu'on sait des pratiques : *DPI or not to be*

Pour ma part, c'est la lecture cet été d'un article d'un spécialiste du SIGINT qui tient un blog appelé Electrospaces qui m'a fait tilter. Il y explique que la police néerlandaise, en chasse contre des hackers russes qui faisaient de la fraude bancaire sur Internet, ont recouru à des techniques de Deep Packet Inspection sur l'infrastructure d'un gros hébergeur hollandais utilisée dans le cadre de ces infractions. La nature de l'outil pose question, puisque le DPI permet de rentrer en profondeur et donc de voir le contenu non chiffré des communications – de *toutes* les communications, y compris celles de personnes sans lien avec l'infraction. Mais c'est la logique qui est intéressante : pour retrouver leurs cibles, les policiers néerlandais sont partis de plus de 400 identifiants utilisés par des cybercriminels russes déjà connus pour voir s'ils les retrouvaient dans le trafic de l'hébergeur.

Or, ces identifiants, quels sont-ils ? Ce sont des logs-ins, ou des pseudos, utilisés par les suspects sur un service de messagerie instantanée appelé ICQ. Les sondes DPI permettaient donc de déceler ces identifiants dans le trafic de l'hébergeur. Ce sont bien des métadonnées qui sont visées : pas celles des opérateurs néerlandais, ni celles de l'hébergeur en question, mais celles de services utilisés en sous-couche dans les paquets de données traités par l'hébergeur.

C'est suite à cela que je suis retourné voir les **révélations faites l'an dernier par Mediapart et Reflets.info sur des sondes DPI du prestataire Qosmos** qu'auraient fait installer les services intérieurs de renseignement français sur l'infrastructure des quatre grands FAI français (programme IOL, sachant que dans le même temps, la DGSE installait un système similaire sur les câbles internationaux, le marché avec Qosmos portant cette fois le nom de Kairos).

Citons en détail un article paru sur Reflets :

> Selon des documents que *Mediapart* et *Reflets* ont pu consulter et les personnes qui ont accepté d'évoquer IOL, il s'agit d'un projet d'interception « légale » chez tous les grands opérateurs, soit à peu près 99% du trafic résidentiel. Ce projet a été imaginé en 2005. Le cahier des charges terminé en 2006 et le pilote lancé en 2007. La généralisation à tous les grands opérateurs s'est déroulée en 2009. Dans le cadre de IOL, des « boites noires » avant l'heure étaient installées sur les réseaux des opérateurs, mais ceux-ci n'y avaient pas accès. Il s'agissait d'écoutes administratives commandées par le Premier ministre et dont le résultat atterrissait au GIC.
>
> Selon un document interne de Qosmos, dimensionné pour permettre de l'interception sur 6000 DSLAM [équivalent du central téléphonique pour l'ADSL], IOL, pour Interceptions Obligatoires Légales, pouvait analyser jusqu'à 80 000 paquets IP par seconde. Un DSLAM pouvant accueillir à l'époque entre 384 et 1008 lignes d'abonnés, c'est entre 2,3 et 6,04 millions de lignes qui étaient alors concernées par ce projet pour la seule société Qosmos. Du massif potentiel (…).
>
> Dans le cas d'IOL, l'outil décrit permettrait d'intercepter les communications électroniques d'un quartier, d'une ville, d'une région ou un protocole spécifique. Ce n'est pas du systématique, comme le fait la NSA, mais c'est une capacité d'interception qui peut très vite glisser vers du massif qui a été installée en cœur de réseau chez tous les grands opérateurs. Les mots ont un sens… « Quelques faucons dans les cabinets ministériels se sont dit qu'il y avait matière à mutualiser l'infra existante pour faire de l'analyse de trafic à la volée, ils ont vu que dans la série « 24 heures » ça se faisait… », indique un brin acide un responsable d'un opérateur qui a vécu l'installation du projet.

Sur Mediapart, Jérôme Hourdeaux insiste bien sur le fait que, malgré le terme d'« interception », ce sont les métadonnées qui sont visées par ces outils, sans toutefois pouvoir préciser lesquelles (mais Qosmos se vante du fait que ces sondes permettent de flasher toutes sortes de protocoles et de données qui donnent des informations extrêmement détaillées sur les activités des internautes, et notamment les sites visités ou l'utilisation de Tor). Le journaliste ajoute également : « 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. »

Le propos se veut rassurant, mais la source ne semble pas avoir été très disserte sur le sujet… Reflets.info relaie les mêmes informations. Toujours selon leurs sources :

> Cette infrastructure était inopérante pour du massif. Pour plusieurs raisons : « L'une étant l'évolution des infrastructures, une autre étant le volume important du trafic chiffré et enfin, la dernière étant qu'il existe une grosse différence entre un démonstrateur (une maquette) et la vraie vie.

Ailleurs dans l'article, la question de l'état actuel de cette infrastructure de surveillance reste ouverte. Selon Reflets : « Qosmos indique s'être retirée du marché de l'interception légale en 2012. Qui entretient aujourd'hui l'infrastructure technique IOL mise en place ? Mystère… ».

Résumons : dans les DSLAM des grands opérateurs télécoms, des sondes DPI ont été expérimentées pour intercepter des métadonnées « piochées » dans le trafic. Or, au départ, en 2009, ces engins semblent avoir été autorisés en vertu de la mesure de surveillance réputée la plus intrusive autorisée en droit français : les interceptions de sécurité (et donc l'interception de tout le trafic d'une cible, métadonnées et contenu compris, l'équivalent d'une écoute téléphonique pour Internet qui, rappelons-le, englobe bien plus que des communications interpersonnelles, mais dont une partie du trafic est effectivement chiffré). Comme le remarquent à l'époque les journalistes, il s'agit bien de sollicitation du réseau en temps réel, et donc de ce qu'a légalisé en 2013 la LPM. Sauf que dans la LPM, il n'est plus question d'interceptions de sécurité, mais de l'accès aux « seules » métadonnées.

Cela pose deux questions :

- Celle de la base juridique avant 2013, d'abord. Il faut savoir que l'une des limites des interceptions pour les services est que la loi plafonne à un peu plus de 2000 le nombre d'interceptions de lignes que les différents services de renseignement peuvent pratiquer en simultané. Une limite qui a des raisons sans doute budgétaires, mais aussi politiques, car ce quota permet de limiter le recours à ces pratiques très intrusives.

  Or, l'accès aux données de connexion n'est pas soumis à un tel plafond. Ce qui invite à faire l'hypothèse suivante : les sondes IOL ont pu rapidement été utilisées pour faire de la surveillance en temps réel des données de connexion, avec comme base juridique non plus les interceptions de sécurité, mais à la fois la loi de 2006 (accès aux données de connexion pour le terrorisme) et d'un article, le L. 244-2, datant de 1991 détourné, qui permettait aux services, pour « la défense des intérêts nationaux » (c'est-à-dire tout et n'importe quoi) de « requérir des opérateurs » les informations et documents, soi-disant en vue de réaliser une interception, le tout sans qu'aucune autorisation préalable ne soit nécessaire ! Par ce détour, les services pouvaient donc s'émanciper du quota et commencer à massifier le nombre de données de connexion ciblées en temps réel avec leurs sondes Qosmos. C'était très bancal juridiquement, d'où la nécessité de faire adopter rapidement la LPM pour consacrer le principe d'un accès en temps réel plutôt qu'*a posteriori*, pour toutes les missions incombant aux services et non plus la seule lutte antiterroriste.
- Deuxième question : quelles sont les métadonnées auxquelles la LPM permet d'accéder à travers les sondes IOL placées sur les réseaux des FAI ? Les journalistes ne s'étendent pas trop là-dessus (peut-être est-ce clair pour eux, compte tenu de la nature des outils DPI ?).

S'agit-il seulement des métadonnées traitées ou conservées par les FAI ? Logiquement, en droit, on aurait tendance à dire que oui. Sauf que des interprétations illogiques sont possibles : on a vu que la LPM puis la loi renseignement parlent systématiquement des données traitées ou conservées par les FAI *ou* les hébergeurs. Tout est mis dans le même sac. Rien ne dit clairement que, pour accéder aux métadonnées des FAI, il faille aller voir les FAI ; que pour accéder à celles des hébergeurs, il faille demander aux hébergeurs.

2.3 Repérer les métadonnées des hébergeurs dans le trafic des opérateurs

Du coup, mon interprétation est la suivante. **Les services peuvent, directement depuis les réseaux des FAI et via ces sondes installées dans les DSLAM, scanner légalement l'ensemble du trafic à la recherche de ces identifiants**, ou « sélecteurs », comme dans l'exemple néerlandais.

Pour passer de l'interprétation « naïve » à la seconde interprétation, il a suffit de se rendre compte que **la loi est suffisamment ambiguë pour permettre aux services de rechercher les métadonnées des hébergeurs dans le trafic des opérateurs**. Ou, en d'autres termes, que la loi ne va pas clairement dans le sens de l'interprétation dominante calée sur la réalité technique, à savoir que les métadonnées des hébergeurs sont en réalité le contenu du trafic des opérateurs – que, pour user d'une analogie postale, la loi n'interdit pas que l'« enveloppe » gérée par les hébergeurs soit accessible depuis les réseaux des opérateurs, quand bien même celle-ci représente pour eux du contenu qu'ils ont pour mission d'acheminer d'un point à l'autre de leurs réseaux.2

Tout le monde – ou presque : des gens comme l'ancien ministre Jean-Jacques Urvoas, le Conseil d'État ou le Conseil constitutionnel font encore de la résistance – considère aujourd'hui que surveiller les métadonnées, ça n'est pas en tant que tel moins intrusif que de surveiller du contenu. De plus, la métadonnée, c'est une notion toute relative. Le plus souvent, la métadonnée d'un intermédiaire technique constitue le contenu des communications acheminées par un autre.

La faille juridique béante à côté de laquelle nous somme passés jusqu'à présent tout en tournant autour en permanence, c'est le fait que la loi ne dit pas clairement à quel endroit de l'infrastructure les services peuvent accéder à quelles métadonnées. Il est ainsi possible de cibler des identifiants associés à un service en ligne, qu'il va s'agir de repérer à la volée dans le trafic à l'aide d'une sonde installée dans un DSLAM – par exemple, quelle IP utilise tel protocole de chiffrement suspect, au hasard Tor. Avouons que c'est quand même beaucoup plus pratique, et moins cher, de traiter directement avec quatre opérateurs télécoms (peut-être un peu plus) pour surveiller en temps réel l'ensemble des données de connexion des hébergeurs, plutôt que d'avoir à s'adresser à des entreprises américaines les unes après les autres.

2.4 Le gouvernement gourmand

Après avoir débattu avec les amis Exégètes de cette lecture, ils sont retournés lire les décrets d'application de la loi renseignement. Et ils se sont rendus compte que, **plutôt que de résoudre l'ambiguïté législative, le gouvernement avait choisi de l'exploiter jusqu'au bout**. Ainsi, à travers le décret n°2016-67, a été créé l'article R. 851-5-1. Cette disposition réglementaire se départit des décrets de 2006 et de 2011 pour définir les données de connexion accessibles en temps réel ou *via* les boîtes noires (article L. 851-2 et L. 851-3). Ces données sont celles :

- Permettant de localiser les équipements terminaux ;

- Relatives à l'accès des équipements terminaux aux réseaux ou aux services de communication au public en ligne ;
- Relatives à l'acheminement des communications électroniques par les réseaux ;
- Relatives à l'identification et à l'authentification d'un utilisateur, d'une connexion, d'un réseau ou d'un service de communication au public en ligne ;
- Relatives aux caractéristiques des équipements terminaux et aux données de configuration de leurs logiciels.

Rien que ça… Le gouvernement réintroduit des **définitions des catégories de données concernées encore plus vagues qu'avant** (la CNCTR elle, refuse d'en dire plus sur ce que recouvre précisément ces catégories, invoquant le secret défense), **il fusionne deux régimes réglementaires qui étaient auparavant définis de manière distincte**, et là encore, tout le monde ou presque était passé à côté (et ce même si la volonté du gouvernement d'élargir le champ des données de connexion était apparue au détour d'un avis de la CNCTR sur les décrets et avait fait débat).

Grâce aux Exégètes, on verra prochainement si le Conseil d'État estime cette disposition réglementaire conforme à la Constitution. Mais cette nouvelle découverte, qui sera détaillée dans un mémoire en cours de finalisation, tend à confirmer la lecture proposée ici : tout en jouant de l'ambiguïté, la LPM puis la loi renseignement, et plus encore un des décrets d'application de celle-ci, ont eu pour but de légaliser l'usage des sondes DPI pour le trafic Internet français. Et ce décret, en fusionnant les deux catégories de métadonnées (FAI / hébergeurs), a pour effet de conforter l'interprétation de la loi selon laquelle les métadonnées traitées par les hébergeurs peuvent être scrutées à partir du réseau des FAI via ces sondes (pour les services, cela a le mérite de la clarté, notamment au cas où un FAI ou un hébergeur s'opposerait à l'installation du DPI sur son réseau en arguant du fait qu'il n'est tenu de permettre l'accès qu'à « ses » métadonnées).

2.5 Qu'est-ce qu'une cible ?

Cette interprétation du couple droit/technique est également confortée par la découverte d'une autre faille juridique de la loi renseignement, dont je ne crois pas qu'elle ait été abordée jusqu'ici, et qui pourrait nous réserver des surprises à l'avenir.

Selon Reflets, toujours sur les sondes Qosmos :

> Si la bonne utilisation était, selon les documents de Qosmos, plutôt de définir une cible, et de donner pour instruction à l'ensemble des sondes de repérer et collecter le trafic de cette cible, était-elle, forcément humaine ? Si la cible est par exemple un réseau social ou un type de comptes mails (Yahoo Mail, Gmail,…), ou encore un protocole (IRC, SIP, Jabber…), on peut très vite franchir une ligne rouge.
>
> D'autant que le document de Qosmos précise qu'il est possible de définir comme cible… des plages d'adresses entières. Et pas seulement des plages de 254 adresses IP… Le document évoque des classes B, soit 65 534 IPs simultanées. Insérer une telle fonctionnalité (qui permet du massif) pour ne pas s'en servir semble pour le moins incongru.

Là, l'auteur fait l'hypothèse que la notion de cible a pu renvoyer à l'interception de tout le trafic en direction d'un gros fournisseur de service, par exemple Gmail, à l'échelle d'un ou plusieurs DSLAM

(dont le trafic Gmail de milliers de personnes). Il rappelle à cet égard que, dans le paramétrage de ces outils, il était possible de scanner le trafic non pas d'un seul abonné (défini par son adresse IP), mais de dizaines de milliers d'abonnés simultanément.

Or, il y a un bout dans la loi renseignement dont on n'a pas assez parlé : dans le 6° de l'article L. 821-2 qui décrit ce que doivent contenir les demandes d'autorisation envoyées pour avis à la CNCTR pour toute mesure de surveillance, il est écrit que chaque demande doit préciser « la ou les personnes visées ».

Juste en dessous, il est précisé : « pour l'application du 6°, les personnes dont l'identité n'est pas connue peuvent être désignées par leurs **identifiants** ». La manière dont on lit ça d'habitude, en mode naïf, c'est que les services ont obtenu d'une manière ou d'une autre soit nom et prénom, soit une adresse IP. Sur cette base, ils obtiennent ensuite une autorisation d'interception correspondant à cet abonné, puis vont poser une « bretelle » pour intercepter son trafic dans le DSLAM le plus proche de son point d'accès. Et effectivement, cela peut correspondre à plusieurs personnes, puisque dans le cas d'une entreprise, d'une association, ou tout simplement d'un foyer, plusieurs personnes utilisent le même abonnement. D'où cette idée qu'une demande de surveillance ciblée puisse viser plusieurs personnes. Circulez il n'y a rien à voir.

Vraiment ?

Une autre lecture est possible. Selon cette lecture, **dans les autorisations, la ou les cibles peuvent être désignées par un ou plusieurs « identifiants »** – en pratique des métadonnées traitées soit par les FAI – par exemple une adresse IP ou une adresse MAC –, soit par les fournisseurs de service – des protocoles spécifiques, voire une adresse mail, un pseudo, un mot de passe, etc. Ces identifiants sont autant de « sélecteurs » permettant de viser non pas des personnes véritablement, mais des patterns de communication dignes d'intérêt pour les services. En renvoyant à des identifiants plutôt qu'à des abonnés, **la loi permet d'élargir la logique exploratoire des boîtes noires aux interceptions, et d'ainsi contourner la limitation de la disposition « boîtes noires » à la lutte antiterroriste.**

En résumé, avec cette lecture, qui abolit la distinction métadonnées du FAI / métadonnées des hébergeurs, autorise le recours au DPI :

- La LPM puis la loi renseignement ont ainsi radicalement transformé la base juridique des utilisations possibles des sondes DPI, en permettant de sortir cette forme de surveillance très intrusive des quotas associés aux interceptions.
- Cette forme de surveillance des données de connexion permet en théorie de dresser beaucoup plus facilement la cartographie sociale d'un individu (non seulement quels serveurs il visite, les services qu'il utilise mais aussi, à supposer que ces identifiants ne soient pas chiffrés, avec qui il échange des mails, converse sur les réseaux sociaux et autres forums, quels sont ses mots de passe, etc.).
- La détection *via* les boîtes noires (article L. 851-3) permet donc bien de faire depuis les réseaux des FAI ce que Le Drian et Bajolet expliquaient au printemps 2015 (sans cibler un individu particulier, paramétrer l'ensemble des sondes posées sur les 6000 DSLAM pour repérer des « comportements suspects » à l'échelle du territoire).

- Hors du champ du terrorisme, une surveillance exploratoire du même type est légalement possible via les interceptions de sécurité (L. 852-1) : sur cette base juridique qui autorise à surveiller le contenu des correspondances et les métadonnées à la fois, les services peuvent en effet choisir de se concentrer uniquement sur ces dernières en utilisant les sondes DPI. Cela semble cependant ne plus être possible pour la surveillance en temps réel, pour laquelle l'article L. 851-2 parle de « personnes préalablement identifiées » en lien avec une menace terroriste et, désormais, d'autorisations accordées « individuellement » pour l'entourage de ces personnes. Ce vocable fait notamment suite à notre QPC remportée dans ce dossier cet été, le gouvernement ayant amendé la loi sur le terrorisme du 30 octobre 2017 pour soumettre cette disposition à un contingentement (quotas), et ainsi l'aligner sur les interceptions de sécurité.

Bref, **cette lecture permet d'expliquer beaucoup de choses qui restaient un peu floues**, même si bien des questions demeurent sur l'interprétation précise des dispositions (par exemple, quelle est la jurisprudence de la CNCTR concernant la nature ou le nombre maximal de cibles pouvant être désignées dans une autorisation ? Pour les interceptions de sécurité « exploratoires », une seule autorisation suffit-elle pour rechercher ces sélecteurs dans l'ensemble des sondes ou faut-il une autorisation par DSLAM/opérateur/… ?).

Ce qui est sûr, c'est que lu à cette lumière, **le droit français contredit l'esprit de la jurisprudence de la Cour européenne des droits de l'Homme**. Cette dernière indique en effet dans une affaire récente (affaire Zakharov) que « le contenu du mandat d'interception *doit désigner clairement la personne précise* à placer sous surveillance ou l'unique ensemble de locaux (lieux) visé par l'interception autorisée par le mandat » (§264). Elle ajoute en outre que le contrôle des autorisations « doit être à même de vérifier l'existence d'un soupçon raisonnable à l'égard *de la personne concernée*, en particulier de rechercher s'il existe des indices permettant de la soupçonner de projeter, de commettre ou d'avoir commis des actes délictueux ou d'autres actes susceptibles de donner lieu à des mesures de surveillance secrète, comme par exemple des actes mettant en péril la sécurité nationale » (§260).

3. Illustrations : hypothèses sur le fonctionnement du couple droit/technique

À partir de tous ces développements, j'essaie dans cette partie d'illustrer les conséquences techniques et opérationnelles de cette interprétation du droit, en tâchant de garder à l'esprit la contrainte que représente l'augmentation du trafic chiffré ces dernières années, puisqu'il tend à masquer un grand nombre de métadonnées très signifiantes pour les services (notamment celles des grandes plateformes).

3.1 Scénario hors lutte antiterroriste

Les services envoient leur demande d'autorisation au premier ministre, qui saisit la CNCTR pour avis. Ils indiquent en substance que les **perquisitions** effectuées sur le matériel informatique d'un individu condamné pour violence volontaire contre les forces de l'ordre lors des manifestations contre la loi Travail montrent qu'il a communiqué avec X *via* Signal. « On suspecte X de prendre part à un groupe de *black bloc* et on a de fortes raisons de penser qu'il est situé dans une zone

géographique proche d'un de ces 20 DSLAM, qui correspondent à la ville dans laquelle le groupe en question se réunit. »

En réponse à cette demande d'autorisation, la CNCTR délivre vingt autorisations d'**interceptions de sécurité « exploratoires »**, soit une par DSLAM sur la zone considérée, sachant que chaque sonde peut être paramétrée pour surveiller des milliers d'IP. Grâce aux sondes installées dans ces DSLAM, les services cherchent des adresses IP ayant pour caractéristiques d'utiliser fréquemment les protocoles Signal et Tor et de consulter plusieurs serveurs caractéristiques des milieux visés. Ils identifient ainsi rapidement trois adresses IP suspectes.

Une autorisation de la CNCTR permet de procéder à l'identification des abonnés correspondant à ces 3 adresses IP (**accès administratif aux données de connexion du FAI qui a atttribué les IP** en question). Elles relèvent toutes les trois du même abonné (IP dynamique). Le suspect est identifié comme Camille George, habitant au 3 rue de la Libération à Nantes. Après avoir envisagé d'aller sonoriser l'appartement du suspect – pratique légalisée par la loi renseignement –, les services préfèrent procéder à une nouvelle interception. Cette fois, on connaît précisément la cible, et ce n'est plus une surveillance exploratoire mais une **interception détaillée de ses communications téléphoniques et Internet**. Deux autorisations d'interceptions sont délivrées par la CNCTR pour quatre mois renouvelables.

3.2 Scénario lutte antiterroriste

Les services ont arrêté deux individus suspectés de projeter un attentat dans un quartier de Marseille. Ils ont saisi leur matériel informatique et ont récupéré des pseudos des contacts Facebook avec lesquels ils ont échangé des messages instantanés. Ils ont des raisons de penser que certains de ces individus leur ont apporté un soutien en France, tandis que d'autres sont en Syrie et ont rejoint l'EI. Ces communications Facebook passent toutes par des serveurs de l'entreprise situés hors du territoire national, et entrent donc dans le champ des communications transfrontalières visées dans les dispositions sur la **surveillance internationale** (lesquelles permettent à la DGSE d'intercepter largement le trafic IP transfrontalier et d'exploiter tant les métadonnées que le contenu des messages, le cas échéant après l'avoir déchiffré).

Déjà autorisée à surveiller toutes les communications des personnes situées en Syrie en direction des serveurs de Facebook au fin de lutte contre le terrorisme, la DGSE met immédiatement en place une **surveillance exploratoire** visant à repérer les communications stockées et déchiffrées impliquant ces identifiants, pour tenter de repérer toutes les communications mentionnant ces pseudos, ainsi que toutes les autres métadonnées associées à ces paquets IP (adresses mails, compte Twitter, etc.). Grâce aux outils *Big Data* mettant en rapport ces différents sélecteurs, la DGSE dresse rapidement le graphe social de ces personnes.

Cela confirme que plusieurs de ces identifiants correspondent à des personnes situées en Syrie. Grâce au trafic intercepté et déchiffré, la direction technique de la DGSE est capable de faire ressortir le contenu de plusieurs messages Facebook échangés par ces personnes avec leurs correspondants. Ces messages laissent notamment apparaître un identifiant utilisé sur un forum prisé des milieux terroristes, mais aussi les noms et prénoms de quatre personnes résidant en France.

Pour ces résidents français, c'est la DGSI qui prend le relais. Après l'envoi de requêtes aux principaux FAI français, on dispose désormais des noms, prénoms et adresses de ces quatre abonnés suspects. L'IP d'une de ces personnes a déjà été **repérée à plusieurs reprises comme ayant voulu se connecter à des sites censurés par l'OCLTIC3** (le blocage du site permet en effet de rediriger l'ensemble des requêtes de consultation vers un serveur du ministère de l'Intérieur, et donc de relever des IPs suspectes). Pour cette IP là, la DGSI demande au Ministre qui sollicite l'avis de la CNCTR pour pouvoir passer directement à **une interception détaillée de ses communications téléphoniques et Internet.** Accordé.

Pour les trois autres abonnés, on passe alors à une **surveillance en temps réel du trafic Internet et téléphonique des abonnés**. En quatre mois, une seule de ces IP laisse apparaître des identifiants caractéristiques des milieux terroristes, notamment le protocole du service de messagerie Whatsapp combiné à des IP de serveurs dont on sait qu'ils hébergent des sites faisant l'apologie du terrorisme.

La DGSI veut se concentrer sur les communications Whatsapp de cet abonné. Grâce à une nouvelle **autorisation « boîtes noires »** (L. 851-3), les sondes à travers le territoire sont paramétrées pour retrouver d'autres paquets contenant le « protocole Whatsapp » de même taille que ceux émis par la cible, et ainsi **les corréler rentre eux**. On arrive ainsi à repérer certaines des IP correspondant à 12 résidents français avec qui la cible communique *via* Whatsapp, dont l'un d'entre eux est fiché S. La DGSI demande une interception ciblée du trafic Internet et téléphonique de ce dernier, qui ne fait plus l'objet d'une surveillance active depuis plusieurs mois.

Les 11 autres personnes sont mises sous surveillance en temps réel pendant quatre mois (la loi autorisant la surveillance des n+2 depuis juillet 2016, la CNCTR n'a plus de bonne raison de s'opposer à cette surveillance). Une seule de ces 11 lignes laisse apparaître des communications « suspectes ». Pour l'abonné en question, une interception ciblée est pratiquée. Pour les 10 lignes restantes, la DGSI ne renouvelle pas les autorisations et arrête donc la surveillance, mais **conserve à toutes fins utiles les métadonnées récoltées pendant trois ans**, tel que la loi l'autorise, dans les bases de données moulinées par les algorithmes de Palantir (le prestataire *Big Data* de la DGSI depuis fin 2016, notamment pour faire sens des masses de données issues des perquisitions réalisées dans le cadre de l'état d'urgence).

Conclusion

Cette interprétation du droit montre que les boîtes noires soi-disant opérationnelles depuis un mois ne sont pas sorties d'un chapeau. De fait, le renseignement français expérimente depuis des années les logiques de surveillance exploratoires, sondant en profondeur le trafic pour repérer des métadonnées suspectes, et s'est même taillé des règles juridiques sur mesure pour s'y adonner « légalement » sans trop éveiller l'attention.

Au plan juridique, cette analyse permet de comprendre **pourquoi le contournement de la jurisprudence de la CJUE sur les métadonnées** – laquelle confirme que la surveillance des métadonnées constitue une ingérence différente mais qui n'est pas de moindre ampleur que celle induite par la surveillance du contenu des correspondances – **constitue une véritable affaire d'État** (Macron a été immédiatement sensibilisé au dossier une fois arrivé au pouvoir, et le Conseil d'État en 2014 allait jusqu'à conseiller d'adopter un protocole interprétatif à la Charte des droits

fondamentaux pour contourner cette jurisprudence de la juridiction suprême de l'UE). La CJUE s'oppose également au fait de surveiller – même « passivement » – les communications de personnes sans lien avec une infraction. Là encore, cela s'oppose aux logiques décrites ci-dessus.

De même, au plan technique, on comprend mieux **pourquoi le chiffrement déployé ces dernières années par les gros fournisseurs de services pose tant de problème au renseignement**, et pourquoi après chaque attentat, le droit au chiffrement est mis en cause – avec en ligne de mire, notamment l'objectif de forcer ces plateformes (Google, Facebook, Twitter et compagnie) à ajuster leurs pratiques en la matière pour ne pas gêner ces formes de surveillance exploratoire (par exemple en s'assurant que les métadonnées qu'ils traitent restent en clair ?).

Bien sûr, compte tenu du secret et des informations parcellaires dont nous disposons, les déductions proposées ici doivent être prises avec des pincettes, et surtout discutées, corrigées, affinées. En pratique, ces systèmes ne sont peut être pas au point pour fonctionner en « grandeur nature » sur un réseau décentralisé comme le réseau IP français, avec désormais plus de la moitié du trafic chiffré, mais qu'en sera-t-il à l'avenir ?

Cela montre en tout cas l'urgente nécessité de faire la transparence sur la nature des outils utilisés par les services de renseignement en matière de surveillance, mais aussi sur l'interprétation que font les services et les autorités de contrôle du droit existant.

Notes de bas page :

- 1. Cet article, devenu depuis 2015 l'article L. 871-2, permet aux services de solliciter des « informations ou documents » en vue de réaliser une interception. Le rapport indiquait que les services faisaient alors environ 30 000 requêtes par an en vertu de la loi de 2006 (donc dans le cadre de la lutte antiterroriste), contre près de 200 000 requêtes sur la base de cette autre dispositions détournée, et couvrant cette fois-ci l'ensemble du champ d'intervention des services de renseignement – et donc des notions aussi vagues que « la sécurité nationale » ou « la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France ». À peu près tout et n'importe quoi, en somme.
- 2. Un exemple pour illustrer ce point : j'envoie un email à une amie. Pour mon FAI, mon adresse mail (felix@lqdn.fr) et celle de ma destinataire (sara@gafa.com) sont du contenu, il n'en a pas besoin pour acheminer mes paquets de données. Pour nos fournisseurs de messagerie en revanche, ceux qui hébergent nos mails, nos adresses mail sont bien des métadonnées, ces identifiants sont nécessaires pour que l'on puisse s'échanger nos messages.
- 3. Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) est l'organisme de la police française dédié à la lutte contre la cybercriminalité.