IFREI

Document de travail

Contenu :

1 Projet de Loi Relatif au Renseignement : Divergences et disparités de perceptions
V2.f 22 avril 2015

2 Annexes :

Vulnérabilité du texte : hébergeurs et disparités topologiques
30 avril 2015

Données, informations, connaissances : la triple relativité de l'information dans la Société de l'information
27 avril 2015

Diffusion :

Auteur :

Pascal Cohet (IFREI)

Contact :

via le site IFREI : http://www.ifrei.org/tiki-contact.php

Remarque liminaire

Ce document de travail ne comporte pas d'analyse partisane, il repose principalement sur une analyse cindynique du second ordre, étudiant les points de vue relatifs des différents acteurs considérés, et les relations entre ces points de vue.

Ce dossier comporte un article initial étudiant la situation conflictuelle (le spectre de situations relatives) créée par le projet de loi relatif au renseignement, ainsi que des annexes, ajoutées au fur et à mesure des besoins ou opportunités. La dernière version de ce dossier est toujours téléchargeable à cette adresse : http://ifrei.org/tiki-download_file.php?fileId=78.

Si la situation est intéressante en raison de la fonction stratégique impactée et des enjeux sociétaux soulevés, l'idée initiale de cette étude est de tenter de publier un texte le plus 'déjargonisé' possible. L'exercice de style, peu aisé, a été suggéré par les retours sur l'article précédent, consacré à l'article 13 du projet de loi de programmation militaire, mentionnant la difficulté qu'éprouve le lecteur profane à décrypter le vocabulaire issu des descriptions cindyniques.

L'objectif est donc d'évaluer la possibilité de publier des études cindyniques 'transparentes' aux Cindyniques pour les lecteurs, sans en altérer la signification. Il n'est pas tout à fait atteint en l'état actuel de ce dossier : certains passages, quoique relativement brefs, pourraient être réécrits/développés en français courant, et certains mécanismes n'ont pas été décrits.

Quoi qu'il en soit, il semble qu'au-delà de la diffusion des modélisations cindyniques en direction des spécialistes, le fait de diffuser des études transparentes aux modèles utilisés pour l'analyse renforcerait la communicabilité, et donc la diffusion des Cindyniques au-delà de la communauté des cindyniciens.

P. Cohet
27 avril 2015

Pour approfondir :

Loi de Programmation Militaire 2014-2019 : Eléments d'évaluation du risque législatif lié à l'article 13

Extension du concept vulnérabilité/résilience : Opérateurs de conformation, conflictualité et conciliance des situations infocindyniques.

Cindyniques et Art de la guerre, Infocindynique et Ultraguerre : La convergence cachée des sciences du danger et de la pensée stratégique chinoise.

Approche infocindynique des crises financières et économiques : Lutte cognitive, étiologie des situations ante-crises et opérateurs de transformation pré-catastrophique.

Black swans, red herrings : Analyse infocindynique d'un scénario de bifurcation des cyber-luttes.

Disparités de perception et divergences prospectives : prévention et résolution de conflits, maîtrise des risques, et développement

Projet de Loi Relatif au Renseignement : Divergences et disparités de perceptions

Pascal COHET [†]

« … aux exégètes amateurs qui comblent leurs lacunes par des préjugés et à ceux de mauvaise foi pour qui le soupçon tient lieu de raisonnement, il faut opposer une analyse dépassionnée du droit. »

Jean-Jacques Urvoas[1]

« Toutefois, la commission estime que les catégories de données qui pourront être demandées devraient figurer dans le présent projet de décret d'application, et non dans un simple arrêté tarifaire… »

Isabelle Falque-Pierrotin[2]

Le projet de loi relatif au renseignement prévoit l'accès ciblé préventif par les services, pour des motifs majeurs comme la prévention du terrorisme, aux données de connexion et à celles d'identification des contributeurs, en particulier en temps réel, ce qui provoque une forte opposition. Cette opposition ne semble pas toujours (vouloir) savoir que ces données sont déjà, depuis plusieurs années, enregistrées préventivement et systématiquement pour l'ensemble de la population française, pour des finalités telles que la répression d'infractions mineures ou de simples téléchargements. Si cette lacune peut être (partiellement) comblée, il n'en reste pas moins que cette tache est d'autant plus ardue que les textes existants ou en débat sont d'une clarté toute relative, et le sont d'autant plus pour le présent projet de loi qu'il est encore plus difficile de réglementer clairement des activités par nature « secrètes ». Dès lors, et quoi qu'il en soit, toute ambigüité résiduelle se surajoutant aux fortes ambigüités caractérisant traditionnellement les textes existants est une source de risque et, partant, d'inquiétude légitime.

Le cas particulier des hébergeurs nécessite un suivi spécifique, et une évaluation du niveau de risque lié tenant compte des levées d'ambigüités [*]*.*

Situation globale

Le projet de loi relatif au renseignement (PLR) présenté mi-mars est un texte majeur et novateur qui assurera un cadre réglementaire aux services dits « secrets », et permettra de prendre en compte les évolutions des techniques et des usages, renforçant notamment de ce fait la prévention du terrorisme.

Le texte, examiné en urgence, doit faire face à une opinion marquée au plan international par les révélations d'Edward Snowden dévoilant l'ampleur des pratiques intrusives du renseignement anglo-saxon, et au plan national par les événements de janvier 2015.

Contrairement à ce qui s'est passé à l'époque du projet de loi de programmation militaire (LPM) dont les dispositions relatives aux communications électroniques avaient peu mobilisé pour des raisons précédemment analysées[3], le PLR provoque une opposition relativement active, le débat étant marqué par de fortes divergences en partie dues à des disparités de perceptions symptomatiques d'une difficulté à percevoir la situation réelle dans son ensemble.

La réduction de ces disparités permettrait de réduire ces divergences et de recentrer le débat sur des bases plus solides, mais, eu égard à l'ampleur des déficits cindynométriques à combler, cette réduction nécessaire sera sans doute limitée par la procédure accélérée.

[†] IFREI - Institut de Formation et Recherche sur l'Environnement Informationnel.

[*] Mise à jour du 19 avril. Cf. infra : « Désambiguïsation du 15 avril : conflictualité du spectre de situation**s** ».

Divergences prospectives apparentes

La plupart des associations dénoncent un texte qu'elles estiment liberticide, en particulier en raison des sondes et dispositifs de traitement faisant de la reconnaissance de patterns comportementaux sur les réseaux des opérateurs, et font parfois référence aux pratiques de la NSA et du GCHQ, voire au Patriot Act états-unien .

Amnesty International[4] dénonce : *l'introduction de techniques illégales de surveillance de masse, la création d'une présomption de surveillance légale, les nouveaux champs d'intervention des renseignements définis de façon trop vague, et l'absence de recours effectif pour les victimes de surveillance illégitime devant le Conseil d'Etat.*

Pour la QDN[5] : « *Surveillance des comportements de tous les internautes par les intermédiaires techniques pour détecter les comportements suspects, accès en temps réel aux données de connexion, accès aux contenus des emails et enregistreurs de frappe au clavier, etc : l'éventail des mesures mises aux mains des services administratifs (police, douanes, etc.) sans contrôle du juge est d'une ampleur sans précédent* »

Pour le collectif OLN[6], regroupant entre autres le Syndicat de la Magistrature, la LDH, la QDN, le Syndicat des avocats de France : « *ce projet légalise des procédés d'investigation jusqu'à présent occultes. Mais pour le reste, les assurances données quant au respect des libertés relèvent d'une rhétorique incantatoire et fallacieuse. Et, prétendant que ce projet de loi fait l'objet d'un large consensus, le gouvernement soumet l'examen du projet en procédure accélérée, confisquant ainsi le débat parlementaire.* »

L'ASIC[7] considère que « *le projet de loi met en œuvre des mesures aboutissant à l'instauration d'une surveillance généralisée. En particulier, comme indiqué par le Gouvernement, les services de renseignement souhaiteraient installer des boîtes noires dans les infrastructures des diverses plates-formes d'hébergement de données, que ce soient des plates-formes de vidéos, des forums de discussion, des plates-formes de commerce électronique, des réseaux sociaux, etc., dans le but de collecter des informations.* » et note qu'il *« s'agit bien d'une surveillance généralisée de tous les internautes, d'une analyse permanente du comportement de ces internautes – afin d'identifier des comportements suspects qui feront l'objet ensuite d'enquêtes spécifiques.* » ou encore : « *Le mécanisme de boîtes noires cherchent à mettre en oeuvre une collecte systématique de l'ensemble des internautes, de l'ensemble des contenus qu'ils visitent ou qu'ils regardent et cela en s'affranchissant totalement des garde-fous existants* »

La CGT Paris[8] dénonce « *une loi qui, sous couvert de lutte contre le terrorisme, est certainement la plus liberticide qui soit. Jamais une loi aussi privative de liberté n'aura été proposée, sauf pendant la guerre d'Algérie.* » et la CGT Police[9] Paris dénonce : « *une loi qui, sous couvert de mieux protéger contre le terrorisme, va en réalité être une des plus liberticides jamais votées depuis celle sur l'état d'urgence. Utilisant ainsi les gens qui sont morts pour la liberté d'expression, ou en raison de leur religion, un gouvernement de gauche (!) veut faire passer une loi qui ne va pas seulement concerner le terrorisme, la prolifération d'armes de destruction massive ou encore la contre-ingérence, mais qui va se glisser dans des domaines plus variés tels que les "intérêts majeurs de politique étrangère" et les "violences collectives pouvant porter gravement atteinte à la paix publique".*»

Le juge Marc Trévidic regrette[10] l'absence du juge: « *Ces pouvoirs exorbitants se feront sans contrôle judiciaire. Ne mentons pas aux Français en présentant ce projet comme une loi antiterroriste. Il ouvre la voie à la généralisation de méthodes intrusives, hors du contrôle des juges judiciaires, pourtant garants des libertés individuelles dans notre pays .*»

Le Conseil National du Numérique est[11] *« préoccupé par l'introduction de nouvelles techniques de renseignement, dont certaines peuvent confiner à une forme de surveillance de masse.*» notant que : « *Il ne suffit pas de répéter qu'il ne s'agit pas d'un Patriot Act à la française. Pour s'en assurer, il faut inclure de manière contraignante le principe selon lequel la surveillance de masse, généralisée et indifférenciée, est étrangère à l'Etat de droit.*»

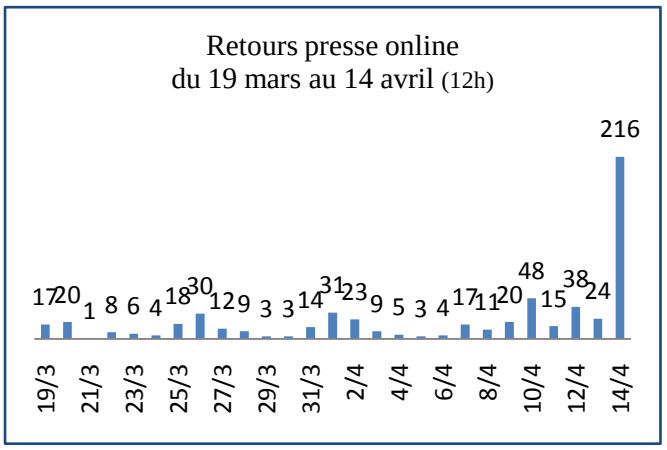
Jean-Marie Delarue[12] s'inquiète de l'usage de dispositifs de type IMSI catcher: « *Par exemple, si vous placez ce dispositif à la gare du Nord pendant six mois - à savoir la durée maximale prévue par le texte - ce sont les données de plusieurs millions de personnes qui pourront être collectées et conservées pendant cinq ans.* »

La réaction des hébergeurs est en revanche plus inquiétante : Gandi note que[13] « *Parmi les dispositions mises en cause par la Commission Numérique et Libertés, la "boite noire" est celle qui nous a le plus interpelés.* », et un collectif[14] (OVH, Gandi, AFHADS, IDS, Ikoula, Lomaco et Online) menace de délocaliser ses activités d'hébergement pour ne pas perdre de clients.

Dynamique des flux de mobilisation

« Les journalistes ne sont pas les seuls à ramer. Certains députés eux-mêmes reconnaissent ne pas y piper grand-chose »
Georges Moréas[15]

Traditionnellement, les opérations d'influence publique des cyberactivistes relèvent de l'agitprop : en substance, un noyau d'entités spécialisées dans le domaine cyber, maîtrisant les aspects techniques et législatifs ou juridiques, peu connus en général en raison d'une complexité certaine, mobilise dans un premier temps de grandes associations connexes, qui ne maîtrisent pas ces sujets, mais qui ont une plus forte audience ou reconnaissance.



Passé un certain seuil, la communication de groupe qui s'en suit déclenche, si elle est suffisamment synchrone, un certain nombres d'articles dans les médias, l'objectif étant d'avoir des retours dans des grands médias généralistes, à forte audience, même si les contenus qu'ils diffusent sont approximatifs. En effet, seuls quelques journalistes suivent régulièrement ces questions, ceux-ci se retrouvant d'ailleurs *ipso facto* aussi prescripteurs que le noyau de cyberactivistes initiant ces opérations d'agitprop, aiguillant ainsi les débats vers telle ou telle direction, par exemple par offuscation, que ce soit volontairement ou non. Le résultat final est souvent peu informatif ou didactique pour le public, la priorité n'étant pas à la formation approfondie du public, mais à la maximisation à court terme de la puissance d'influence.

Pour autant, le PLR a suscité d'emblée de nombreux retours presse, sans doute en raison de l'image romantique ou cinématographique couramment associée à tout ce qui touche au renseignement, ce qui facilite une large mobilisation autour du débat, indépendamment de la qualité qui lui serait nécessaire.

La réaction des hébergeurs est caractérisée par une menace particulièrement vive de délocalisation, mais, en se référant au rapport Urvoas, *si* celui-ci ne comporte pas d'erreur, il apparaît qu'il est possible qu'ils ne soient pas forcément concernés et qu'il y ait une erreur de rédaction dans le texte du PLR : ce problème sera spécifiquement abordé.[*]

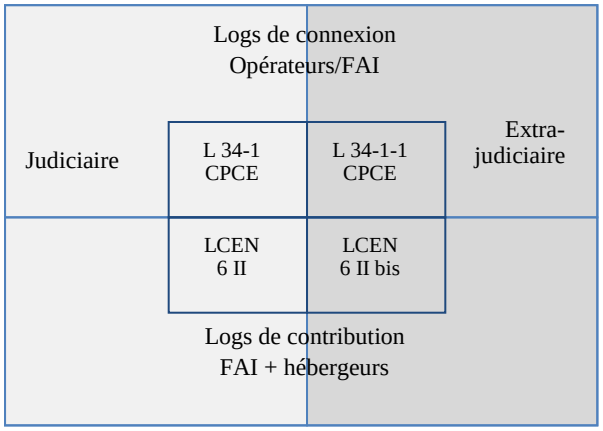
Nécessité d'élargissement de l'horizon de la situation

« Sans vouloir nourrir votre réflexion halieutique collective, je dirais que la pêche à la ligne est ciblée, que la pêche au chalut est globale, et que la pêche à la senne fait dans le global ciblé. »
Gilbert Le Bris[16]

Une part importante des réactions des cyberactivistes au PLR indique une méconnaissance manifeste de l'histoire, qui tient sans doute au renouvellement du tissu associatif ou à l'apparition d'une nouvelle génération d'activistes qui n'ont pas connu les débats qui ont eu lieu depuis la fin des années 90. La structuration progressive et maillée - dont l'histoire fait sens- des divers textes touchant à la réglementation des TIC, ainsi que la pervasivité de l'ambigüité des définitions juridiques n'aident pas les néophytes à appréhender l'ensemble de ce complexe de problématiques. Une synthèse du processus progressif de structuration des lois a déjà été faite à l'occasion de la LPM dans un article précédent[17], mais ces lacunes nécessitent un rappel schématique des points essentiels :

La loi française prévoit deux types de surveillance d'internet : les logs de connexion (données de connexion des internautes), et les données d'identification des contributeurs (logs de contribution destinés à retrouver les internautes qui créent, modifient, ou suppriment un contenu sur l'internet public). Les logs sont recueillis par les opérateur de communications électroniques *dont* les fournisseurs d'accès à internet (FAI), et les données d'identification sont recueillies par les FAI et les hébergeurs.

[*]Cf. infra, mise à jour du 19 avril : « Désambiguïsation du 15 avril : conflictualité du spectre de situations ».



L'accès à ces données (de connexion ou d'identification) peut être judiciaire, ou extrajudiciaire (administratif). Dans ce dernier cas, il arrive fréquemment que des acteurs réclament (parfois consciemment, par simple posture) l'intervention du juge ('gardien des libertés') même s'il s'agit de réglementer des activités administratives.

Cet accès extrajudiciaire aux données de connexion et d'identification des contributeurs (le fameux « bloc extrajudiciaire expérimental », temporaire) est désormais pérennisé dans le code de la sécurité intérieure (CSI) : c'était justement tout l'objet du fameux article 13 (désormais 20) de la LPM dont le débat fin 2013 a été peu ou pas suivi par les cyberactivistes.

Pour le judiciaire, les logs de connexion sont prévus par l'article L 34-1 du code des postes et des communications électroniques (CPCE) issu historiquement de l'article 29 de la loi relative à la sécurité quotidienne (LSQ) à la suite du 11 septembre, et le recueil des données d'identification des contributeurs par le II de l'article 6 de la loi pour la confiance dans l'économie numérique (LCEN) elle-même issue, après de vifs débats, en 2004 de la tardive transposition de la directive commerce électronique (2000/31 CE).

D'après le L 34-1 du CPCE ces logs sont requis :

«Pour les besoins de la recherche, de la constatation et de la poursuite des *infractions pénales* ou d'un manquement à l'obligation définie à l'article L. 336-3 du code de la *propriété intellectuelle* ou pour les besoins de la prévention des *atteintes aux systèmes de traitement automatisé de données* prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire ou de la haute autorité mentionnée à l'article L. 331-12 du code de la propriété intellectuelle ou de l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense »

Motifs d'accès aux logs de connexion (L34-1 du CPCE)	Autorité pouvant accéder aux logs de connexion
Infractions	Autorité judiciaire
Téléchargements	HADOPI
Atteinte SI	ANSSI

Pour l'extrajudiciaire, les logs de connexion étaient prévus par le L 34-1-1 du CPCE, créé en 2006 par l'article 6 de la loi relative à la lutte contre le terrorisme (LCT) dénoncé à l'époque par une seule cyberONG, qui n'a pas été suivie médiatiquement, et pour qui, point important, le fait de loguer préventivement l'ensemble de la population française n'était pas acceptable, la seule surveillance acceptable devant cibler uniquement des individus raisonnablement suspects. Le recueil extrajudiciaire des données d'identification des contributeurs a quant à lui été instauré par le même article 6 de la LCT, via la création d'un II bis à l'article 6 de la LCEN. Ce bloc extrajudiciaire est désormais codifié dans les articles L246-1 et suivants du CSI, le L 34-1-1 du CPCE ainsi que le II bis de l'article 6 de la LCEN ayant été abrogés.

Plus en détail, plusieurs décrets ont tendu à préciser ce que sont ces données de connexion ou d'identification des contributeurs (certains acteurs considèrent que l'habitude qui consiste à garder des textes flous et rejeter ces précisions à des décrets ultérieurs nuit à la clarté du débat démocratique, d'autres, tel le SGDSN[18], peuvent considérer que ce flou rend la loi plus souple vis à vis des évolutions des techniques et des usages, et d'autres encore que le flou juridique est une source manifeste de risques).

En ce qui concerne les logs judiciaires, instaurés en 2001, c'est le décret 2006-358 (donc 5 ans plus tard) qui a précisé via la création des articles R 10-12 à R 10-14[19] du CPCE la nature des données devant être enregistrées préventivement pour une durée de un an (ils doivent ensuite obligatoirement être effacés), soit, en substance :

- *Les informations permettant d'identifier l'utilisateur ;*
- *Les données relatives aux équipements terminaux de communication utilisés ;*
- *Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;*
- *Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;*
- *Les données permettant d'identifier le ou les destinataires de la communication.*

S'agissant des FAI, qui constituent un sous-ensemble des opérateurs de communications électroniques, la signification des mots 'destinataire' et 'communication' pose un problème de compréhension.

En ce qui concerne l'enregistrement des données d'identification des contributeurs instaurés en 2004 pour le judiciaire et en 2006 pour l'extrajudiciaire, c'est le décret 2011-219[20] (donc respectivement 7[21] et 5 ans plus tard) qui a précisé la nature de ces données, devant être conservées durant un an, soit, en substance :

pour les FAI :

► *L'identifiant de la connexion*
► *L'identifiant attribué par ces personnes à l'abonné*
► *L'identifiant du terminal utilisé pour la connexion lorsqu'elles y ont accès*
► *Les dates et heure de début et de fin de la connexion*
► *Les caractéristiques de la ligne de l'abonné*

pour les hébergeurs :

► *L'identifiant de la connexion à l'origine de la communication*
► *L'identifiant attribué par le système d'information au contenu, objet de l'opération*
► *Les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus*
► *La nature de l'opération*
► *Les date et heure de l'opération*
► *L'identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a fourni*

pour les FAI et les hébergeurs :

► *Au moment de la création du compte, l'identifiant de cette connexion*
► *Les nom et prénom ou la raison sociale*
► *Les adresses postales associées*
► *Les pseudonymes utilisés*
► *Les adresses de courrier électronique ou de compte associées*
► *Les numéros de téléphone*
► *Le mot de passe ainsi que les données permettant de le vérifier ou de le modifier, dans leur dernière version mise à jour*

La récupération des mots de passe des utilisateurs fait douter certains acteurs du bienfondé de l'affirmation selon laquelle la récupération des *données* ne concernerait pas les *contenus* des utilisateurs. De même, certains acteurs, au premier rang desquels les professionnels concernés, voire leur autorité de régulation[22], peuvent estimer que certaines de ces précisions ne sont pas démunies d'un certain flou sémantique qui pose un problème très concret dès lors qu'il s'agit de respecter 'en pratique' une obligation légale.

La plupart des données d'identification des contributeurs sont des données *statiques*, hormis pour la date/heure d'opération devant être retenue par les hébergeurs (ce qui pose un problème spécifique dans le cadre du PLR), et la date/heure de connexion devant être retenue par les FAI (et, dans ce dernier cas, la signification du mot 'connexion' est possiblement plus problématique que ce qui est couramment admis). S'agissant du bloc extrajudiciaire pérennisé dans le CSI, l'expression « informations ou documents » posait un problème de définition, et comme prévu[23], même si le Président de la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat avait déjà dû préciser[24] cette signification, le décret 2014-1576[25] est venu confirmer via la création de l'article R 246-1 du CSI que dans ce cas les informations ou documents sont « *à l'exclusion de tout autre* » : pour les logs, les mêmes que celles définies par le décret 2006-358, et pour les données d'identification des contributeurs, les mêmes que celles définies par le décret 2011-219.

Textes définissant les données concernées	Logs de connexion et de contribution Accès judiciaire (L 34-1 du CPCE, et LCEN 6II)	Informations ou documents Accès extrajudiciaire (Article 20 LPM)
Décret 2006-358	Logs de connexion	Logs de connexion
Décret 2011-219	Logs de contribution	Logs de contribution

Ce contexte juridique et historique élargi étant posé, il est alors possible d'y situer le débat nécessaire à la bonne compréhension du PLR sur des bases décrivant plus complètement le réel, permettant de relativiser les dispositions prévues par rapport aux dispositifs existants, et de mieux évaluer les proportionnalités, la question de la proportionnalité étant cruciale pour toute problématique d'horogénèse informationnelle.

Articles conflictuels du projet de loi relatif au renseignement

« J'ai l'habitude de dire que le renseignement, c'est cochon, et tous les gens qui se retrouvent à ma place vous diront à peu près la même chose. »
Christian Prouteau[26]

Par rapport au cyberespace, il faut considérer au sein du PLR principalement l'article 1, créant le L 811-3 du CSI (définition des missions), et l'article 2 qui crée dans ce même code : le L 851-1 (renumérotation du L 246-1 existant), le L 851-3 (sondes) et le L 851-4 (algorithmes de détection des signaux faibles, qui soulèvent de vives inquiétudes), le L 851-5 (ex L 246-3) et le L 851-7 (dispositifs de proximités : « IMSI » catchers).

Missions

Le L 811-3 précise les missions des services de renseignement à l'occasion desquelles ils peuvent être amenés à utiliser les dispositifs prévus par le PLR :

► *La sécurité nationale*
+► *Les intérêts essentiels de la politique étrangère et l'exécution des engagements européens et internationaux de la France*
► *Les intérêts économiques et scientifiques essentiels de la France*
► *La prévention du terrorisme*
► *La prévention de la reconstitution ou du maintien de groupement dissous en application de l'article L. 212-1*
► *La prévention de la criminalité et de la délinquance organisées*
+► *La prévention des violences collectives de nature à porter gravement atteinte à la paix publique*

Le L 851-1, renumérotation du L 246-1 *déjà existant* dans le CSI, fait référence aux missions du L 811-3, sensiblement élargies par rapport au L 241-2[27], et prévoit le recueil des 'informations ou documents' auprès des opérateurs de communications électroniques dont les FAI (*mentionnés* au L 34-1 du CPCE) et auprès des FAI et des hébergeurs (les personnes du 1 et du 2 de l'article 6 de la LCEN).

Les missions prévues au L 241-2 étaient :

► *La sécurité nationale,*
► *la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France,*
► *la prévention du terrorisme,*
► *la prévention de la criminalité et de la délinquance organisées*
► *la prévention de la reconstitution ou du maintien de groupements dissous en application de l'article L. 212-1*

Sondes

Le L 851-3 prévoit le recueil *en temps réel*, uniquement pour la prévention du terrorisme, des 'informations ou documents' concernant un *nombre limité de personnes préalablement identifiées* auprès des *personnes mentionnées au L 851-1.*

Description dans l'étude d'impact[28] : «La simple sollicitation *a posteriori*, auprès des opérateurs, de certaines données techniques de communication relatives à des personnes surveillées – ce que permet l'actuel L. 246-1 du code de la sécurité intérieure – n'est pas suffisante pour disposer d'une appréhension globale en temps réel.
C'est pourquoi, l'article L 851-3 autorise, pour les besoins de la détection précoce d'actes de terrorisme, la collecte, en temps réel, sur les réseaux des opérateurs, de la totalité des données, informations et documents relatifs aux communications de personnes préalablement identifiées comme des menaces. Contrairement à ce qu'il en est des personnes surveillées au titre des interceptions de sécurité, le contenu de leurs communications ne sera en aucun cas intercepté. Seules les données de connexions seront recueillies sur le fondement de ce nouvel article. »

Description dans le rapport Urvoas : « En outre, là où les services américains interceptent et stockent massivement des données personnelles puis sollicitent des autorisations pour exploiter les informations conservées, à l'inverse, le texte prévoit que les services vont solliciter préalablement des autorisations de collecte extrêmement précises et ciblées sur des individus représentant une menace avérée.

C'est le cœur du nouvel article L. 851-3 du code de la sécurité intérieure (3° du II de l'article 2), qui prévoit que, pour les seuls besoins de la prévention du terrorisme, les services de renseignement peuvent recueillir, en temps réel, les informations et documents mentionnés à l'article L. 851-1 du code de la sécurité intérieure (1) relatifs à des personnes préalablement identifiées comme présentant une menace, sur les réseaux des opérateurs de téléphonie et des fournisseurs d'accès à internet. Il s'agit donc de permettre un accès instantané aux seules données de connexions (ce qui exclut l'accès au contenu même des échanges, à laquelle seule une interception de sécurité permettra d'accéder) pour une liste limitative de personnes présentant un risque en matière de terrorisme (ce qui suppose de détenir au préalable un faisceau d'indices concordants sur la dangerosité des personnes concernées). »

Remarque : Si le L 851-3 ne prévoit que du recueil ciblé en temps réel -pour la prévention du terrorisme- d'informations ou documents, c'est-à-dire de données de connexion (définies par le décret 2006-358) et de données d'identification de contribution (définies par le décret 2011-219), ces deux catégories de données sont (du fait du L 34-1 du CPCE et du II de l'article 6 de la LCEN) par ailleurs systématiquement enregistrées (loguées) par les opérateurs de communications électroniques, les FAI et les hébergeurs. Ces logs sont accessibles *a posteriori* aussi par les services du fait du L 851-2.

Détection des signaux faibles

Le L 851-4 prévoit, lui aussi uniquement pour la prévention du terrorisme, de pouvoir imposer aux *personnes mentionnées au L 851-1* un algorithme de reconnaissance de patterns (détection de menaces terroristes) sur les 'informations ou documents' *anonymes (ce qui exclut donc une partie des données prévues au décret 2011-219).*

Description dans l'étude d'impact : «Afin d'identifier le plus en amont possible l'existence de ces menaces, les services de renseignement, confrontés à une multitude sans cesse croissante de réseaux, modes et supports de communications générant au plan planétaire des flux massifs de données, doivent pouvoir recueillir, traiter, analyser et recouper un grand nombre d'éléments techniques anonymes pour détecter les signaux de faible intensité qui témoignent d'une menace pesant sur les intérêts de notre pays.

Il convient de dépasser l'approche exclusivement fondée sur le suivi de cibles déjà connues ou repérées pour privilégier la recherche d'objectifs enfouis sous le maquis des réseaux de communications transnationaux, Internet offrant à cet égard des opportunités de furtivité immenses pour les acteurs et vecteurs de la menace.

Opérée grâce à la détection anonymisée de certains comportements de communication, cette détection sera prévue par le nouvel article L. 851-4 du code de la sécurité intérieure. La levée de l'anonymat pesant sur les données collectées, qui serait justifiée par la révélation de la réalité d'une menace, ferait l'objet de la procédure de droit commun d'autorisation par le Premier ministre après avis de la commission de contrôle. »

Description dans le rapport Urvoas : « De la même manière, le nouvel article L. 851-4 du code de la sécurité intérieure ouvre la possibilité, pour les services de renseignement, d'imposer aux opérateurs téléphoniques et aux fournisseurs d'accès à internet de mettre en place un algorithme qui détecterait une menace terroriste, mais ce, sans procéder à l'identification des personnes concernées par l'analyse des données autres que celles suspectées de terrorisme.

L'objectif poursuivi est donc bien, pour l'État, de pouvoir recueillir, traiter, analyser et recouper un grand nombre d'éléments techniques anonymes pour détecter des signaux de faible intensité sur les données brutes qui témoigneraient d'une menace pesant sur la sécurité nationale. Cette disposition n'impose donc pas aux prestataires de services sur Internet une « obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites », ce que prohibe l'article 15 de la directive sur le commerce électronique (1).

(1) Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur. »

Le L 851-5 reprend le L 246-3 du CSI créé par la LPM, *semblant* destiné à la géolocalisation en temps réel (et non *a posteriori*) : *« Pour les finalités énumérées à l'article L. 811-3, les informations ou documents mentionnés à l'article L 851-1 peuvent être recueillis sur sollicitation du réseau et transmis en temps réel par les opérateurs à un service du*

Premier ministre. » En effet, le rapport Urvoas précise *: « Le nouvel article L. 851-5 du code de la sécurité intérieure (4° du II bis du présent article) reprend les dispositions de l'article L. 246-3 du même code, qui prévoit la possibilité de transmission en temps réel des données de connexions et, donc, de localisation. »*

Le L 851-7[29] prévoit l'utilisation de dispositifs de portée *locale* de type 'IMSI catcher', ce qui inquiète certains acteurs, comme Jean-Marie Delarue, Président de la Commission nationale de contrôle des interceptions de sécurité (CNCIS), pour les cas où ils seraient disposés dans des lieux où le passage du public est important (gare, …).

Avis de la CNIL

La CNIL a publié son avis (Délibération n°2015-078 du 5 mars 2015 portant avis sur un projet de loi relatif au renseignement.[30]) entre autre sur les sondes et les algorithmes de détection de signaux faibles :

Sur les sondes : « La Commission relève tout d'abord que les modalités de recueil (en temps réel et directement sur sollicitation du réseau, sans l'intermédiaire des opérateurs de communications électroniques) constituent une évolution majeure au regard du dispositif prévu à l'actuel article L. 246-3 du CSI. Elle considère que cette nouvelle possibilité est de nature à permettre l'aspiration massive et directe des données par les agents des services concernés sur les réseaux des opérateurs, par l'intermédiaire de la pose de sondes.

Elle s'interroge en outre sur le périmètre exact des données concernées au regard de la formulation retenue, qui ne correspond pas à celle utilisée aux articles L. 851-1 à L. 851-3 (nouveaux) du CSI. Elle estime dès lors que cette formulation devrait être clarifiée afin de préciser, le cas échéant, que seules les données de connexion peuvent être recueillies sur le fondement de ce nouvel article.

Enfin, dès lors que cette mesure ne concerne pas uniquement une personne identifiée mais est susceptible de concerner un ensemble de personnes «*préalablement identifiées comme présentant une menace*», la Commission observe que seule la prévention du terrorisme, et non les autres intérêts publics mentionnés dans le projet de loi, pourra permettre la mise en œuvre de cette mesure, ce qui constitue une garantie substantielle. Au regard du caractère particulièrement intrusif de cette technique et de son utilisation à l'insu des opérateurs, sur leurs propres systèmes, la Commission estime que les garanties prévues pour préserver les droits et libertés fondamentaux ne sont pas suffisantes pour justifier une telle ingérence dans la vie privée des personnes. »

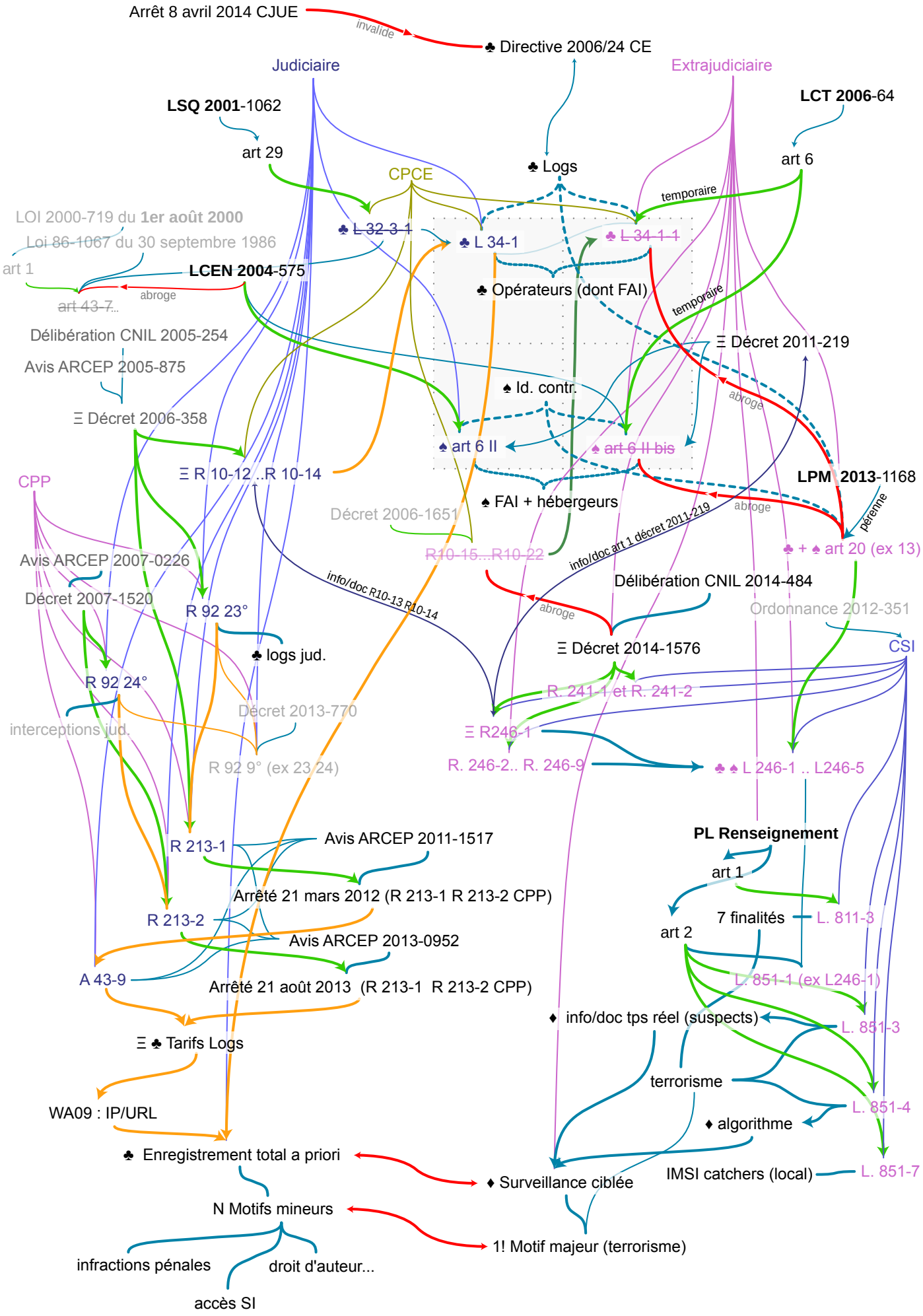
Sur la détection des signaux faibles : « En deuxième lieu, l'article L. 851-2-2 du CSI tel que prévu par le projet de loi prévoit la mise en œuvre, sur les informations et documents traités par les réseaux des operateurs, d'un dispositif destiné à caractériser « *sur la seule base de traitements automatisés d'éléments anonymes, la préparation d'un acte de terrorisme* ». Il est néanmoins prévu que l'anonymat des personnes concernées soit levé « *en cas de caractérisation de menace terroriste* ».

Ces dispositifs visent a détecter des signaux dits faibles de préparation d'un acte de terrorisme, à partir de critères pré-établis portant sur les données détenues par les operateurs. Les « signaux faibles » s'entendent de tendances, de *modus operandi*, ou encore de traces qui risquent d'être illisibles ou non détectables prises isolément, mais qui, rapportés à un ensemble de personnes, mettent en évidence des occurrences révélatrices de certains comportements.

La Commission appelle l'attention du Gouvernement sur la formulation retenue concernant cette disposition : si le traitement automatisé de détection des signaux faibles par les opérateurs n'a vocation qu'à identifier un faisceau d'indices permettant de caractériser une menace terroriste, il n'en demeure pas moins qu'il porte sur des données indirectement ou directement identifiantes et non sur des éléments anonymes, comme le démontre d'ailleurs la possibilité de remonter à l'identité de la personne.

A cet égard, la Commission rappelle que ces traitements devront faire l'objet de formalités préalables, conformément aux dispositions de la loi du 6 janvier 1978 modifiée. Le décret en Conseil d'Etat, pris après avis de la Commission, qui devra préciser les modalités d'application de ces dispositions devra en outre prévoir des conditions de transmission adéquates des données, une fois l'anonymat levé, entre les opérateurs et le service demandeur. »

Structuration partielle simplifiée



Déficits statiques et dynamiques, facteurs de disparités de perception

> *Malgré la mythologie qui m'entoure et le détestable surnom raciste de « SDECE tartare », je suis resté extrêmement loin des opérations que le service Action appelait « Homo » et le grand public « Main rouge ».*
> Constantin Melnik[31]

Accès aux informations et documents / logs de connexion et logs de contribution

Les réactions des divers opposants au PLR font l'objet de nombreux communiqués et articles de presse qui peuvent sembler exhaustifs, néanmoins, un certain nombre de textes déjà existants et importants sont absents de la photo présentée au public. Outre l'impact cindynométrique de ce déficit dynamique, il est surtout éventuellement révélateur d'une importante lacune axiologique. Le processus de mobilisation précédemment décrit présente cette vulnérabilité que si le noyau initial prescripteur est peu nombreux, ou en situation de monopôle, alors toute lacune cindynométrique le caractérisant se propage sans correction vers le grand public, tendant à construire l'opinion publique de façon biaisée, sur une représentation faussée ou incomplète du réel, ce qui est une source de conflictualité inutile.

Resituées dans le contexte juridique existant, les parties concernées du PLR peuvent être intégrées dans un comparatif :

Le L 851-3 vise à recueillir uniquement pour un nombre limité de suspects préalablement identifiés les informations ou documents qui les concernent, uniquement pour la prévention du terrorisme. Ces mêmes (strictement) informations et documents sont en fait déjà recueillis systématiquement pour la totalité des abonnés à internet pour une durée de un an, et accessibles au juge pour des infractions même mineures, ou un simple téléchargement de film ou de musique.

Le L 851-4, uniquement pour la prévention du terrorisme, prévoit d'analyser une partie seulement des informations ou documents puisque les parties non anonymes en sont exclues : ces informations ou documents sont par ailleurs déjà tous enregistrés *a priori*, préventivement, pour tous les abonnés à internet.

Quant au L 851-7, prévoyant des dispositifs de proximité, même si ceux-ci sont placés dans une gare où passent quelques milliers de passagers, ce chiffre doit être comparé à celui des dizaines de millions d'abonnés à internet déjà systématiquement logués par les opérateurs et les hébergeurs.

Textes	Motifs d'accès aux logs de connexion	Autorité accédant aux Logs de connexion
L 34-1 CPCE	Infraction pénale (contravention, délit, crime)	Autorité judiciaire
L 34-1 CPCE	Téléchargement (L.336-3 du code de la propriété intellectuelle)	HADOPI
L 34-1 CPCE	Atteinte SI (323-1 à 323-3-1 du code pénal)	ANSSI
L 851-2 PLR (ex L246-2 CSI)	L 811-3 (dont terrorisme)	Services
L 851-3 PLR	Terrorisme	Services
L 851-4 PLR	Terrorisme	Services

Resitués dans un contexte juridique historique élargi contribuant à combler les lacunes cindynométriques, les dispositifs prévus par le PLR n'apparaissent donc plus comme relevant d'une « mise en place de la surveillance de masse sur internet » perçue par certains activistes[32].

D'un point de vue cindynique, la plupart des oppositions manifestées sont ainsi caractérisées par une très forte dégénérescence téléologique - constituant sans doute un cas d'école qui sera difficilement supplanté - due à d'importantes lacunes cindynométriques, globalement dues à la propagation de flux informationnels toxiques - relayés par des médias traditionnellement déficitaires sur des sujets techniques - issus d'un petit nombre d'acteurs ayant sous-dimensionné l'horizon d'analyse de la situation, et présentant eux-mêmes des déficits statistiques, et épistémiques, voire, possiblement, axiologiques.

La prise en compte du droit existant déjà dans le monde réel permet ainsi de comprendre cette analyse de Jean-Marie Delarue[33] : « *On peut se demander si la police administrative ne devrait pas avoir moins de moyens que la police judiciaire. Je réponds à cela négativement. Compte tenu des dangers auxquels nous sommes exposés aujourd'hui, je ne vois pas de motifs pour lesquels la recherche de l'auteur d'une infraction devrait bénéficier de plus de moyens que la prévention des infractions graves.*»

Cette compréhension élargie de la situation pourrait mener les cyberactivistes à adopter une stratégie différente : la cible prioritaire de l'opposition ne serait plus la surveillance ciblée prévue par le PLR, mais les logs de connexion et d'identification pesant déjà sur l'ensemble de la population, ce qui serait cohérent avec le récent arrêt de la CJUE invalidant la directive 2006/24 CE.

Hébergeurs

En revanche, s'agissant des hébergeurs, il est vrai que la pose de sondes ou de dispositifs algorithmiques de détection pose un problème difficilement compréhensible. Pour autant, il semblerait qu'il y ait un problème rédactionnel, et que le texte ne traduise pas précisément l'intention du législateur : Comme vu précédemment, le L 851-3 et le L 851-4 mentionnent les « personnes mentionnées au L 851-1». Or Le L 851-1, issu des travaux de la commission des lois prévoit :

> « L 851-1 Pour les finalités énumérées à l'article L. 811-3, 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. »

Mais : le rapport de Jean-Jacques Urvoas[34] fait au nom de la commission des lois, enregistré le 2 avril 2015, précise plusieurs fois à propos du L 851-3 et du L 851-4, que ces articles concernent les opérateurs téléphoniques et les FAI :

A la page 42 :
L 851-3 :

> « C'est le cœur du nouvel article L. 851-3 du code de la sécurité intérieure (3° du II de l'article 2), qui prévoit que, pour les seuls besoins de la prévention du terrorisme, les services de renseignement peuvent recueillir, en temps réel, les informations et documents mentionnés à l'article L. 851-1 du code de la sécurité intérieure (1) relatifs à des personnes préalablement identifiées comme présentant une menace, sur les réseaux des opérateurs de téléphonie et des fournisseurs d'accès à internet. »

[…]

L 851-4

> « De la même manière, le nouvel article L. 851-4 du code de la sécurité intérieure ouvre la possibilité, pour les services de renseignement, d'imposer aux opérateurs téléphoniques et aux fournisseurs d'accès à internet de mettre en place un algorithme qui détecterait une menace terroriste, mais ce, sans procéder à l'identification des personnes concernées par l'analyse des données autres que celles suspectées de terrorisme. »

Et aux pages 195-196 :
L 851-3 :

> « Le nouvel article L. 851-3 du code de la sécurité intérieure (3° du II bis du présent article) est une disposition nouvelle. Aux termes de cet article, pour les seuls besoins de la prévention du terrorisme, le recueil des informations et documents mentionnés à l'article L. 851-1, relatifs à des personnes préalablement identifiées comme présentant une menace, peut être opéré en temps réel sur les réseaux des opérateurs de téléphonie et des fournisseurs d'accès à internet. La Commission a adopté un amendement de clarification de votre rapporteur pour souligner explicitement que ce recueil d'informations et de documents fait l'objet d'une procédure d'autorisation.
>
> Il s'agit donc de permettre un accès instantané aux seules données de connexions (ce qui exclut l'accès au contenu même des échanges, à laquelle seule une interception de sécurité permettra d'accéder) pour une liste limitative de personnes présentant un risque en matière de terrorisme. En effet, la simple sollicitation a posteriori, auprès des opérateurs, des entreprises offrant un accès à des services de communication au public en ligne et des fournisseurs d'accès à internet, de certaines données techniques de communication relatives à des personnes surveillées n'est pas suffisante pour disposer d'une appréhension globale en temps réel. »

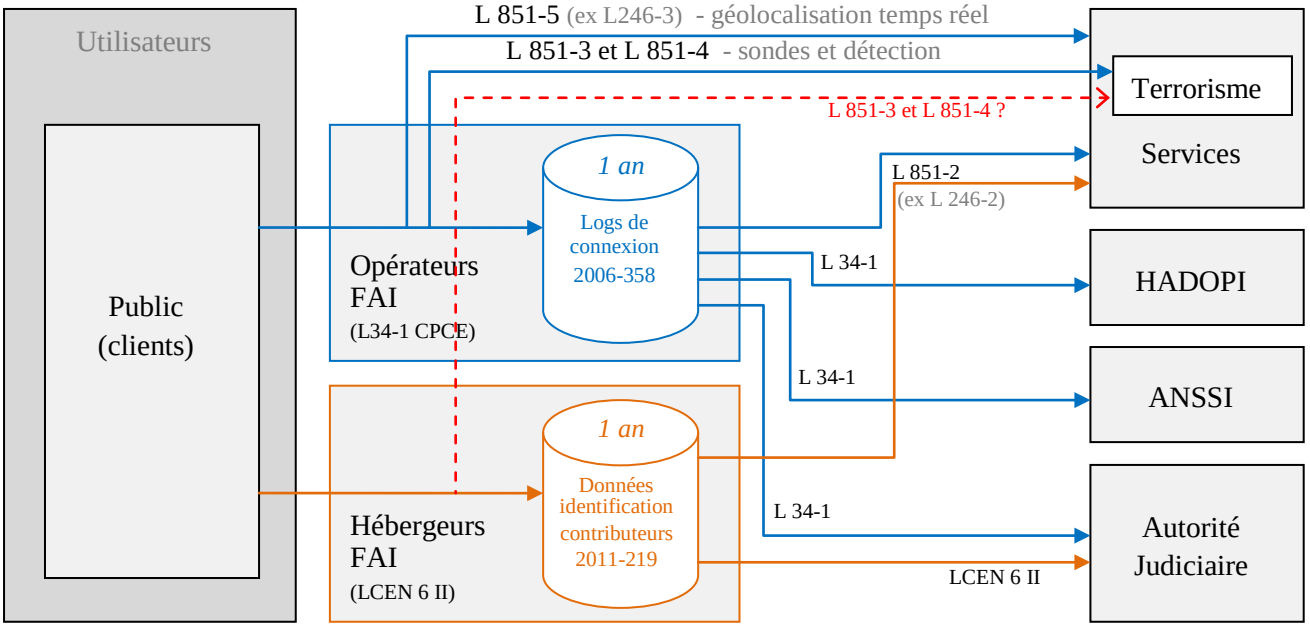
[…]

L 851-4 :

> « Le nouvel article L. 851-4 du code de la sécurité intérieure (3° du II bis du présent article) est également une disposition nouvelle. Aux termes de cet article, pour les seuls besoins de la prévention du terrorisme, sur demande des agents individuellement désignés et dûment habilités des services spécialisés de renseignement, le Premier ministre, ou l'une des personnes déléguée par lui, peut, après avis de la CNCTR, imposer aux opérateurs téléphonique et fournisseurs d'accès à internet la mise en œuvre sur les informations et documents traités par leurs réseaux d'un dispositif destiné à révéler, sur la seule base de traitements automatisés d'éléments anonymes, une menace terroriste. »

Avec tant de précisions spécifiant de façon répétée que ce sont les opérateurs téléphoniques et les FAI qui sont visés, il est possible de comprendre que la mention des « *personnes mentionnées au L 851-1* » dans le L851-3 et le L 851-4 est une simple erreur rédactionnelle qui devrait être corrigée de cette façon : « *personnes mentionnées au L 34-1 du code des postes et communications électroniques* ». Quoi qu'il en soit, ce point mérite clarification[*].

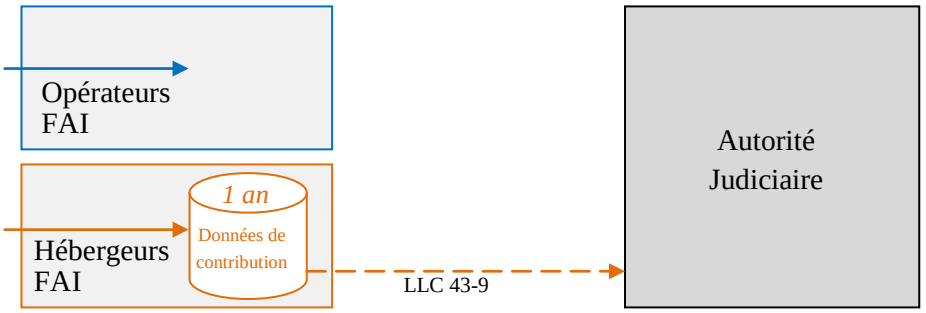
Schéma résumé : accès temps réel (PLR) vs a posteriori (PLR, CPCE, LCEN)



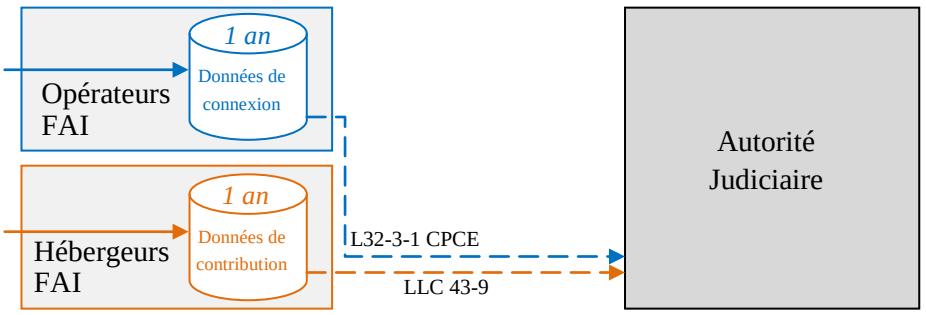
[*] Cf. infra, mise à jour du 19 avril : « Désambiguïsation du 15 avril : conflictualité du spectre de situations ».

« Il y a en tout homme deux êtres : lui-même et l'opinion publique.»
Auguste Detœuf

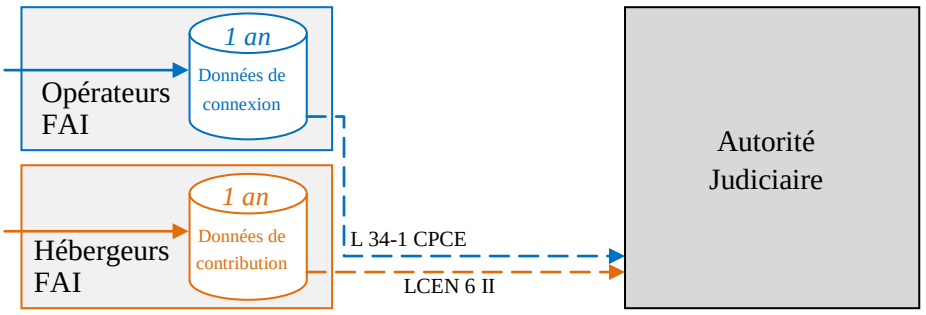
La loi du 1er aout 2000 relative à la liberté de communication (LLC) prévoit par son article 43-9 l'enregistrement de toutes les données permettant d'identifier tous les contributeurs, pour mise à disposition de l'autorité judiciaire.
Décret : mesure non prise par le gouvernement.



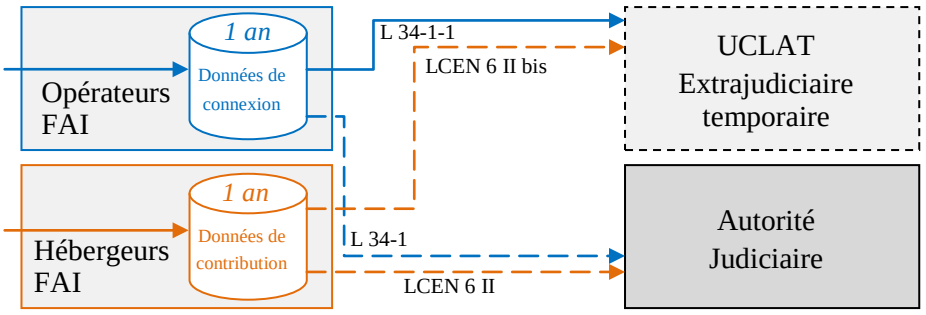
Le 15 novembre 2001, après les attentats du 11 septembre, l'article 29[35] de la LSQ crée le L 32-3-1 du CPCE, imposant l'enregistrement de toutes les données de connexion des internautes, pour mise à disposition de l'autorité judiciaire, dispositif anti-terroriste temporaire, par la suite *pérennisé* par l'adoption en décembre 2002 de l'amendement Estrosi[36] n°86 à la LPSI (Loi n°2003-239).



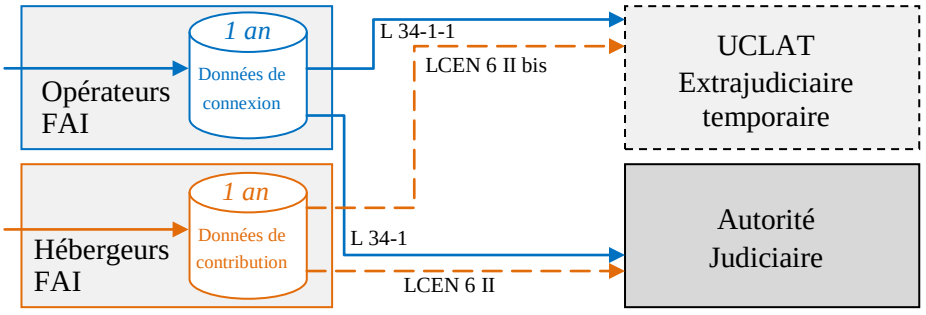
Le 21 juin 2004, le II de l'article 6 de la LCEN reprend les dispositions du 43-9 de la loi du 1er aout 2000. Dans la foulée, le L 32-3-1 du CPCE devient le L 34-1 via l'article 10 de la loi du 9 juillet 2004[37].
Les décrets relatifs aux données de connexion et au données de contribution restent en attente.



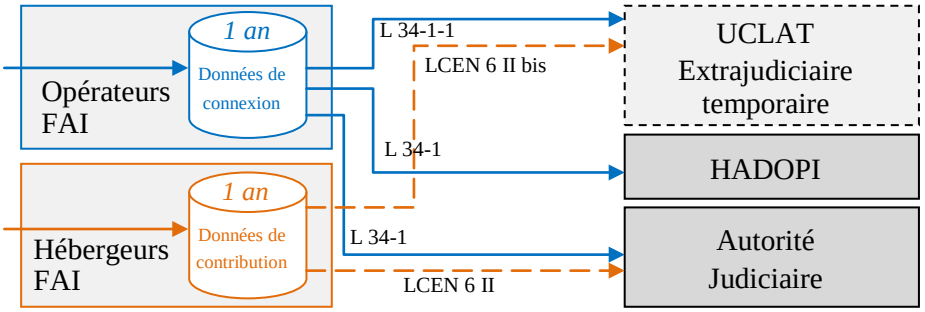
Le 23 janvier 2006, l'article 6 de la LCT autorise *temporairement* un accès extrajudiciaire aux données de connexion par la création du L 34-1-1 du CPCE et aux données de contribution par l'insertion d'un II bis dans l'article 6 de la LCEN. L'article 4 de la LCT *étend* par ailleurs la définition des opérateurs du L 34-1[38].



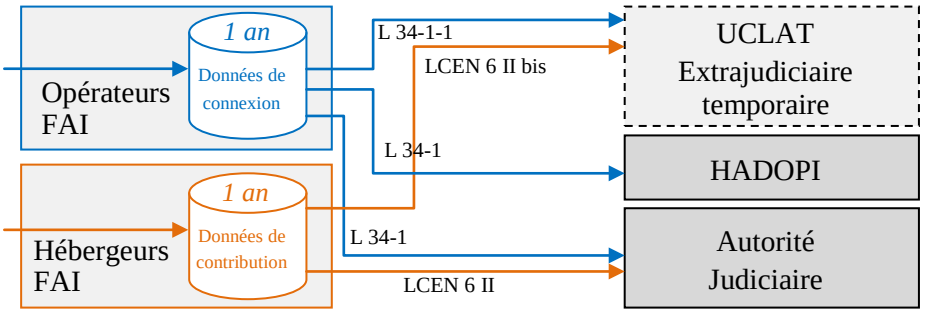
Le décret n° 2006-358 du 24 mars 2006 crée les articles R 10-12 à R 10-14 du CPCE, précisant les données de connexion devant être loguées par les opérateurs mentionnés au L 34-1 du CPCE pour mise à disposition de l'autorité judiciaire.



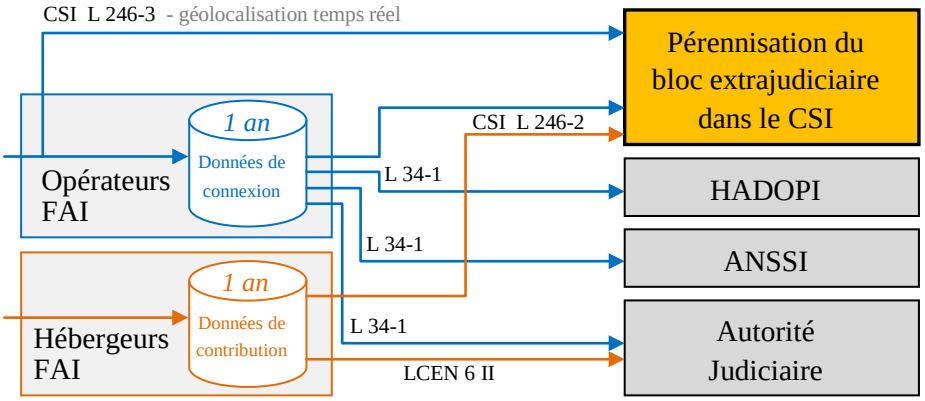
L'article 14 de la Loi n° 2009-669 du 12 juin 2009 dite « HADOPI » modifie le L 34-1 du CPCE en donnant accès aux données de connexion à une autorité chargée de la lutte contre le téléchargement d'œuvres par exemple musicales ou cinématographiques, au motif, issu *in fine* du processus législatif, de 'non sécurisation de son accès internet'.



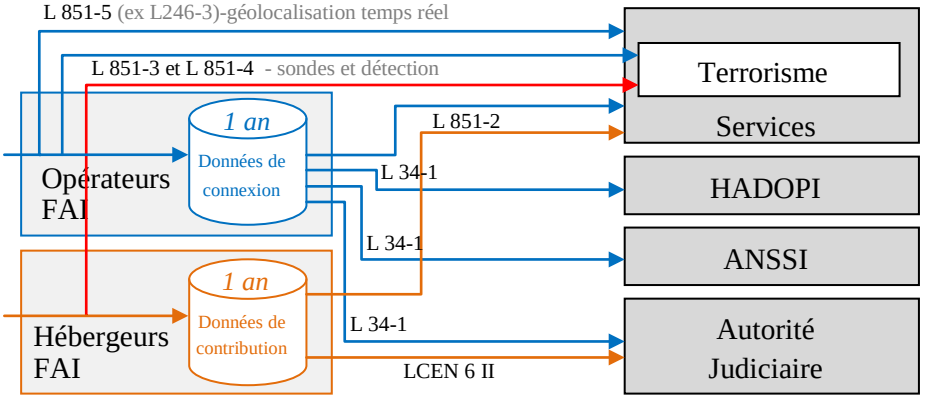
Le décret n° 2011-219 du 25 février 2011 précise les données de contribution devant être loguées par les FAI (personnes mentionnées au 1 du I de l'article 6 de la LCEN) et les hébergeurs (personnes mentionnées au 2 du I de l'article 6 de la LCEN), en application du II et du II bis de l'article 6 de la LCEN.



En décembre 2013 le bloc extrajudiciaire expérimental créé par l'article 6 de la LCT est *pérennisé* par l'article 13 de la LPM, le codifiant dans les articles L 246-1 et suivants du CSI. Les données visées, dites 'informations ou documents', expression ayant soulevé de vives inquiétudes en raison du flou sémantique la caractérisant depuis 1991, regroupent finalement précisément les données de connexion prévues par le décret n° 2006-358 du 24 mars 2006, et les données de contribution précisées par le décret n° 2011-219 du 25 février 2011. Pour autant, les définitions apportées par ces deux décrets ne sont elles-mêmes pas exemptes -à ce jour- d'ambigüités. Dans le même temps, l'accès aux données de connexion est accordé à l'ANSSI, en tant qu'autorité nationale de sécurité des systèmes d'information[39]. L'article L 246-3 créé permet la géolocalisation en temps réel via la récupération des données des opérateurs, auparavant récupérées *a posteriori*. Le champ des acteurs autorisés à accéder aux données, ainsi que les motifs d'accès sont par ailleurs *étendus*[40]. Enfin, l'article 14 (devenu 21) de la LPM, autorise un accès aux PC des internautes (ex. : machine infectée) en cas d'attaque .



Par rapport à la LPM, le PLR introduit donc en fin de comptes relativement peu de nouveautés, soit, notamment : un *élargissement* des motifs d'accès (L 811-3), ainsi que les installations de sondes (L 851-3) et algorithmes (L 851-4) chez les opérateurs, mais aussi, le point étant désormais clarifié - et problématique - chez les hébergeurs (malgré des mentions répétées, dans le rapport Urvoas, aux seuls opérateurs et fournisseurs d'accès à internet) . Du point de vue du cyberactivisme, la mise en place d'une « surveillance de masse extrajudiciaire » date donc en réalité de la pérennisation du bloc extrajudiciaire expérimental par l'article 13 de la LPM en décembre 2013. Mais, en raison de la vulnérabilité créée par son absence de réaction significative[41] à cette époque, la gestion de son risque image lui impose une offuscation par focalisation de sa communication offensive sur les sondes et dispositifs de détection prévus par le PLR, créant par ailleurs ainsi un déficit cindynamique.



La délicate question du tarif WA09 à 15,70€

« Les significations des mots glissent et se tortillent comme des anguilles et elles échappent à l'entendement»
Mioara Mugur-Schächter

Si les acteurs ayant manifesté une opposition au texte sont pour la plupart caractérisés par les déficits cindyniques précédemment cités, le législateur, ou plus exactement la chaîne d'acteurs impliqués dans l'écriture et la validation de la loi présente aussi quelques déficits, en particulier en ce qui concerne l'ambigüité des définitions produites : c'est le cas pour les 'données de connexion', expression dont le flou sémantique pose un problème majeur dès lors qu'il s'agit de lois touchant à des enjeux démocratiques d'une telle importance.

L'ensemble du processus se modélise de façon pertinente avec le modèle Reason : à chaque étape, qu'il s'agisse de la rédaction du projet de loi, du travail des commissions, des amendements, d'une éventuelle saisine du conseil constitutionnel, de la rédaction des décrets, jusqu'à la rédaction de simples arrêtés, les ambigüités cindynogènes persistent. Ainsi, pour les données de connexion, il y a eu en particulier successivement :

1) L'article 29 de la LSQ créant le L 32-3-1 du CPCE,
2) le décret 2006-358 créant les articles R 10-12 à R 10-14 du CPCE,
3) après l'avis 2005-875 de l'ARCEP
4) et la délibération 2005-254 de la CNIL,
5) le décret 2007-1520
6) après l'avis 2007-0226 de l'ARCEP,
7) l'arrêté du 21 mars 2012
8) pris après l'avis 2011-1517 de l'ARCEP,
9) puis l'arrêté du 21 août 2013
10) pris après l'avis 2013-0952 de l'ARCEP
11) et qui met à jour l'article A 43-9 du code de procédure pénale,

C'est donc l'article A 43-9 du CPP qui permet d'avoir *in fine* une idée plus précise des données de connexion prévues par la loi, par le biais de grilles de tarifs de remboursement de frais aux opérateurs, ce 12 ans après l'instauration des logs.

C'est ainsi que l'ARCEP, dans son Avis n° 2013-0952 du 23 juillet 2013 sur les projets d'arrêtés relatifs à la tarification des réquisitions judiciaires, des interceptions de sécurité et la fourniture des données par les opérateurs de communications électroniques mentionne :

> « L'Autorité note que l'objectif principal des deux premiers projets d'arrêtés mentionnés ci-dessus est d'ajouter, à côté des prestations existantes relatives aux données de téléphonie, les prestations et tarifs associés pour les données liées à l'utilisation d'internet. En effet, bien que les articles L. 34-1-1 et R. 10-13 du code des postes et des communications électroniques imposent aux opérateurs la conservation de ces données, les tarifs des prestations dédiées à l'internet n'avaient encore jamais été fixés. Il s'agit de sept prestations dans le cadre des enquêtes judiciaires et de six prestations dans le cadre de la lutte contre le terrorisme. La détermination et la tarification de ces prestations permettent ainsi aux opérateurs de connaître de manière précise et transparente les données qu'ils sont susceptibles de devoir fournir ainsi que les tarifs associés. »

C'est sans doute en raison de l'usage répété de ces procédés que, dans sa Délibération n° 2014-484 du 4 décembre 2014 portant avis sur un projet de décret relatif à l'accès administratif aux données de connexion et portant application de l'article L. 246-4 du code de la sécurité intérieure, la CNIL précise :

> « Il a en outre été indiqué que l'arrêté tarifaire prévu à l'article R. 246-9 nouveau du CSI précisera les différentes prestations de transmission de données de connexion concernées, ce qui inclura nécessairement les catégories de données visées. Toutefois, la commission estime que les catégories de données qui pourront être demandées devraient figurer dans le présent projet de décret d'application, et non dans un simple arrêté tarifaire, et demande dès lors, afin d'éviter toute confusion sur la nature des données concernées, que le projet de décret soit modifié en ce sens. »

De façon intéressante, l'arrêté du 21 août 2013 qui complète les tarifs de remboursement des opérateurs de téléphonie par la grille[42] des « *Tarifs hors taxes applicables à la fourniture de données par les opérateurs de communications électroniques* », qui comporte la ligne suivante :

WA 09	A partir d'une adresse URL de site visité horodatée, obtenir les éléments d'identification relatifs à la personne physique, à l'installation, à la connexion, au contrat et aux identifications numériques.	15,70 €

Ce que semble indiquer ce tarif, c'est que l'opérateur concerné doit indiquer aux autorités quel est l'abonné qui a visité une URL donnée à un instant donné. Ce qui logiquement lui imposerait nécessairement de disposer d'un fichier recensant toutes les URL visitées par tous ses abonnés pour pouvoir en extraire la ligne correspondant à l'URL visitée horodatée fournie par l'autorité et lui transmettre l'identité de l'abonné.

Quoi qu'il en soit, même si l'ARCEP estime que ces tarifs permettent de connaître précisément les données que les opérateurs doivent conserver, il se pourrait que lesdits opérateurs ne l'aient pas compris ou interprété ainsi. Toujours est-il que cet exemple illustre la difficulté que rencontre le public pour décrypter les lois relatives à internet, en l'occurrence, dans ce cas : pour savoir si les URL de tous les sites visités par chaque internaute sont loguées, ou pas. Si certains acteurs estiment parfois qu'une URL est une donnée de contenu, donc exclue des données de connexion par le L 34-1, sans doute en référence à une ancienne publication du FDI sans réelle valeur juridique, sauf erreur, *stricto sensu* aucun texte de loi ne définit ce qu'est une donnée de contenu.

A l'instar des délais de plusieurs années qui se sont écoulés avant que les décrets d'applications prévus par des lois relatives à la lutte anti-terroriste ne soient publiés, l'incertitude engendrée par la persistance des flous sémantiques entourant des définitions pourtant cruciales ne peut que dégrader la confiance accordée au législateur.

Dans ces conditions, et eu égard à l'importance des enjeux démocratiques concernés, même si les oppositions au PLR sont d'une vivacité souvent décalée par rapport à la réalité des textes existants, il est suggéré qu'au-delà des flux didactiques cindynolytiques dont la mise en œuvre est nécessaire pour combler d'importantes lacunes du public, un effort substantiel devrait être fait pour minimiser le risque sémantique et rendre la loi plus intelligible, ce qui est par ailleurs un objectif à valeur constitutionnelle.

Par ailleurs, si la chaîne d'acteurs impliqués dans la rédaction des lois, décrets, et arrêtés est marquée par une tendance au flou sémantique n'aidant pas à éclairer le public, il faut aussi remarquer un déficit comparable chez les opérateurs, FAI et hébergeurs qui pourraient quant à eux publier les champs précis de leurs fichiers de logs, ce qui n'a pas été fait à ce jour. Ces derniers, par exemple ceux manifestant une opposition au PLR, contribueraient de cette façon à éclairer le public, et à la clarté du débat, en exprimant ainsi chacun clairement leur propre interprétation pratique de la loi.

Désambiguïsation du 15 avril : conflictualité du spectre de situations

« pour un stratège, être la cible commune de l'ensemble d'un système dit 'a-téléologique' est peut-être une des pires situations qui soit. »[43]

Avec l'accumulation constante des déficits sémantiques, l'ensemble de l'édifice législatif voit sa vulnérabilité s'accroître, que ce soit au regard de la constitution ou du droit européen. Par ailleurs, ces déficits inquiètent le public, et sont donc intrinsèquement des facteurs d'opposition. Pour autant, c'est une clarification nette qui a accru significativement les divergences prospectives, et donc la conflictualité de la situation :

Comme remarqué précédemment, le cas des hébergeurs nécessite une attention spécifique, pour de nombreuses raisons, de principe, et historiques. Le rapport Urvoas, document de référence permettant d'avoir une idée relativement précise de l'intention du législateur, mentionnait de façon répétée que les sondes et algorithmes concernaient les opérateurs et FAI. Or les hébergeurs ont été reçus[44] le 15 avril au Ministère de l'intérieur, où des détails leur ont été communiqués[45] sur les techniques de renseignement que le gouvernement souhaite mettre en œuvre sur leurs infrastructures. Contrairement à ce que laissait penser le rapport Urvoas, qui s'avère d'ailleurs *ipso facto* porteur d'un déficit cindynométrique, l'article L 851-4 ne sera donc pas limité aux personnes mentionnées au L 34-1 du CPCE.

Si de nombreuses divergences sont actuellement dues aux disparités de perception des acteurs causées par des déficits partagés menant à des difficultés à percevoir le réel, il apparaît maintenant une divergence -majeure- qui elle est due à une certitude concrète : le PLR vise à imposer des dispositifs de détection sur les installations des hébergeurs, quelles que puissent être par ailleurs les modalités prévues par l'adoption de l'amendement 437[46].

Or, il y a pour le cyberactivisme -ultimement- deux choses auxquelles il ne faut pas toucher : un serveur, ou un nom de domaine. A l'instar de la DCRI, marquée par un déficit culturel qui ne lui a pas permis de prévoir l'effet Streisand -par nature trans-frontière- qu'elle allait nécessairement subir en s'attaquant à Wikipedia, le législateur semble avoir méconnu cette caractéristique profonde, pratiquement d'ordre phylogénétique, du cyberespace : le cyberactivisme ne peut tolérer qu'on touche à un serveur. Ainsi, par exemple, la saisie d'un serveur Rackspace à Londres par le FBI avait provoqué il y a quelques années une forte réaction internationale. A l'ère post-Snowden, ce type d'action aurait certainement des conséquences plus larges et plus diverses.

Quoi qu'il en soit, ces divergences sont désormais claires et posées, et d'intensité telle que des opérateurs de transformation vont maintenant probablement s'opposer frontalement. Il ne s'agit plus de débattre ou clarifier, le problème est désormais binaire : retirer ou non cette disposition.

Si une étude plus complète est nécessaire pour caractériser les risques liés à la dynamique de ce spectre de situations, quelques éléments essentiels et de transduction peuvent déjà être remarqués :

Le débat relatif aux hébergeurs, historiquement important en France, et marqué par de vives confrontations, remonte, bien avant la LCEN, à l'affaire Altern. A ce sujet, l'actuel retour sur le devant de la scène de dinos comme Valentin Lacambre ou Laurent Chemla ne peut pas être considéré comme un signal particulièrement faible. Sans surprise, Altern a déjà annoncé sa délocalisation[47]. Pour la dimension économique, il sera important de suivre les décisions des autres hébergeurs, qui dépendront sans doute des attitudes de leur clients, elles-mêmes dépendant de l'intensité et de l'horizon des flux informationnels d'opposition au PLR, y compris à l'international.

Face à ce phénomène de délocalisation, le gouvernement peut espérer que les états-membres adopteront des dispositifs analogues. Ce scenario risque de se heurter aux capacités transnationales du cyberactivisme : il existe des réseaux de coordination qui seront sans doute mobilisés par les français pour étendre l'opposition à une partie de l'Union européenne, et il se pourrait au contraire qu'*in fine* des instances européennes critiquent le dispositif prévu, d'où un possible risque législatif, d'ailleurs contextuellement accru par la récente décision de la CJUE.

Un effet de bord non négligeable de ces flux informationnels à l'échelle internationale est le risque de renforcement des flux axiologiques des mouvances djihadistes : leurs discours pourront se compléter d'éléments présentant la France comme un pays utilisant des méthodes totalitaires vis-à-vis des internautes. Si en général ce type de discours a peu de chances d'être efficace ou crédible, il peut en revanche l'être vis-à-vis de personnes peu résilientes, c'est-à-dire radicalisables. Il y a donc un risque de contre-productivité dans la lutte-anti-terroriste, en particulier pour la prévention de la radicalisation.

Au-delà des dimensions politiques, économiques, informationnelles, législatives, et axiologiques, la dimension LIO pourrait aussi être impactée : La décision d'imposer des dispositifs de renseignement chez les hébergeurs pourrait être un facteur de bifurcation, tel qu'exposé dans un scenario[48] précédemment publié, poussant des entités à s'attaquer de façon persistante à des systèmes d'information français, en synchronisation ou coordination tacite, i.e. sans communication, avec des mouvements activistes s'en tenant eux à des domaines d'action légaux.

Si l'analyse de la dynamique à venir est rendue délicate dès lors qu'elle implique un système a-téléologique ou auto-organisateur -du fait d'ailleurs des déficits épistémiques du cyberactivisme en matière de pensée stratégique- il est toutefois raisonnable de conjecturer que la crise envisagée pourrait être l'une des plus importantes de l'histoire du net français.

P. Cohet.

V2.f 22 avril 2015

Annexe 1 :

Vulnérabilité du texte : hébergeurs et disparités topologiques

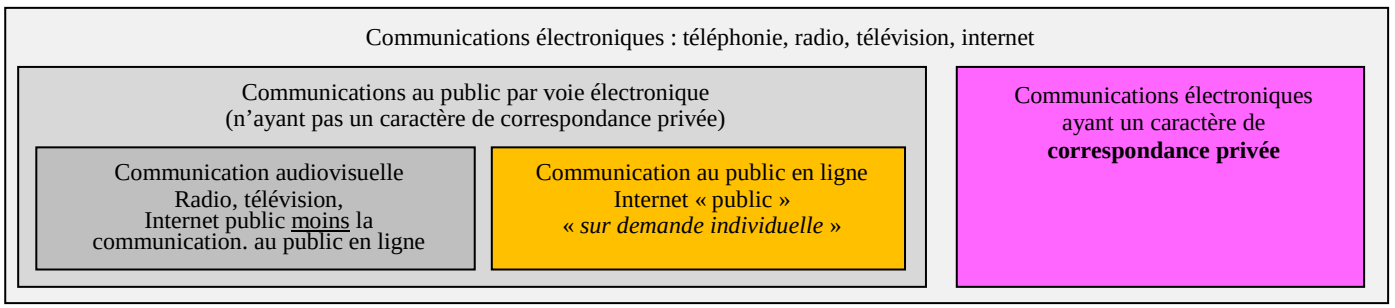
« …la vocation d'une raquette, c'est justement d'avoir des trous.»
Jean-Jacques Urvoas[49]

Si les ambigüités caractérisant constamment le droit des TIC n'en facilitent pas l'herméneutique, l'avancement des débats permet d'avoir progressivement une idée plus précise de l'intention du législateur, en particulier en ce qui concerne le problème de l'impact du PLR sur les hébergeurs. Ainsi, lors d'une conférence à l'ENSP le 18 avril, Jean-Jacques Urvoas[50] a apporté ces précisions :

> «*il y a des opérateurs, il y a des fournisseurs d'accès, et puis il y a des hébergeurs. Et au regard de la loi tous n'ont pas la même responsabilité. Si nous arrivons à nous entendre, un peu sous la contrainte, avec les opérateurs et les fournisseurs, il y a aujourd'hui une résistance des hébergeurs. Les hébergeurs c'est gmail, c'est skype, c'est facebook : "moi monsieur je suis un hébergeur, donc je mets un tuyau en place, ce qui se passe dans le tuyau c'est pas ma responsabilité." Et donc le constat que nous avons fait, que les services ont fait, que les policiers font, c'est qu'on peut continuer à avoir nos écoutes téléphoniques, mais il ne s'y dit plus rien, et que les anticipations, les préparations, les préméditations se font sur d'autres vecteurs, dont l'accès a été rendu encore plus difficile depuis qu'Edward Snowden a fait ses divulgations*».

Il semble donc que Jean-Jacques Urvoas considère Gmail et Skype comme des acteurs faisant partie de l'ensemble des personnes mentionnées au 2 du I de l'article 6 de la LCEN. Or, en l'état, les deux articles les plus conflictuels du PLR, le L851-3 (sondes) et le L 851-4 (algorithmes), visent les « *personnes mentionnées au L 851-1*», c'est-à-dire les opérateurs et FAI (L 34-1 du CPCE), les FAI (personnes mentionnées au 1 du I de l'article 6 de la LCEN), et les hébergeurs (personnes mentionnées au 2 du I de l'article 6 de la LCEN). Historiquement, la notion d'hébergeur est initialement floue, et repose sur une jurisprudence biaisée par la revendication par certains acteurs du statut d'hébergeur, en raison de la protection qu'il offre. Une des critiques portées à l'encontre de la LCEN avant son adoption était justement que les acteurs, en particulier les hébergeurs, n'étaient pas clairement définis, ce à quoi Patrick Devedjian, Ministre de l'Industrie en charge du projet de loi, avait répondu juste avant l'examen du texte par le conseil constitutionnel : « *Effectivement, le texte est perfectible, mais nous aurons l'occasion de revenir dessus* »[51].

L'essentiel des débats de l'époque concernait la responsabilité des hébergeurs, dont il était attendu qu'ils suppriment des *publications* 'illicites' ou 'litigieuses' (et, finalement, 'manifestement illicites'[52]) avant l'intervention du juge. Deux domaines étaient concernés : la communication (injures, diffamation…) et le droit d'auteur (les industries culturelles souhaitant que les hébergeurs retirent les œuvres publiées ou 'mises à disposition' sans leur accord). Parallèlement, le projet de loi prévoyait pour d'obscures raisons[53] de placer internet sous la tutelle du CSA, ce qui avait soulevé une forte opposition[54]. Comme mentionné dans une étude précédente[55] consacrée à la LPM, cette divergence avait été réduite via un amendement[56] des sénateurs Sido et Hérisson établissant une architecture du droit des communications électroniques accordant au CSA un droit de regard sur les 'contenus audiovisuels' *aussi* sur internet, mais *uniquement* sur *ces* contenus internet.



Le fait important ici est que les communications électroniques ayant un caractère de correspondance privée sont du fait de cette architecture clairement exclues de la 'communication au public par voie électronique' :

> « *On entend par communication au public par voie électronique toute mise à disposition du public ou de catégories de public, par un procédé de communication électronique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée.* ».

Et, partant, de la ‘communication au public en ligne’ :

> « *On entend par communication au public en ligne toute transmission, sur demande individuelle, de données numériques n'ayant pas un caractère de correspondance privée, par un procédé de communication électronique permettant un échange réciproque d'informations entre l'émetteur et le récepteur.* »

Or le 2 du I de l’article 6 de la LCEN définit ainsi les hébergeurs :

> « *Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services […]* »

Enfin, historiquement, pour en revenir au droit communautaire à l’origine de la LCEN, la directive commerce électronique[57] précisait clairement :

> (18*) Les services de la société de l'information englobent un large éventail d'activités économiques qui ont lieu en ligne. Ces activités peuvent consister, en particulier, à vendre des biens en ligne. […] Les services de la société de l'information ne se limitent pas exclusivement aux services donnant lieu à la conclusion de contrats en ligne, mais, dans la mesure où ils représentent une activité économique, ils s'étendent à des services qui ne sont pas rémunérés par ceux qui les reçoivent, tels que les services qui fournissent des informations en ligne ou des communications commerciales, ou ceux qui fournissent des outils permettant la recherche, l'accès et la récupération des données. Les services de la société de l'information comportent également des services qui consistent à transmettre des informations par le biais d'un réseau de communication, à fournir un accès à un réseau de communication ou à héberger des informations fournies par un destinataire de services. […] L'utilisation du courrier électronique ou d'autres moyens de communication individuels équivalents par des personnes physiques agissant à des fins qui n'entrent pas dans le cadre de leurs activités commerciales ou professionnelles, y compris leur utilisation pour la conclusion de contrats entre ces personnes, n'est pas un service de la société de l'information. […].*

L’article 14[58] de cette directive définissait ainsi l’hébergement :

> *Hébergement*
> *1. Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le prestataire ne soit pas responsable des informations stockées à la demande d'un destinataire du service à condition que: [...]*

Dès lors, certains juristes, constatant que Gmail et Skype sont des services qui relèvent éminemment de la correspondance privée, pourraient considérer que ce type d’acteurs ne relève *ipso facto* pas du 2 du I de l’article 6 de la LCEN mentionné au L851-1. Ainsi, -sauf à bouleverser l’architecture actuelle du droit des communications électroniques, ce qui représenterait un vaste chantier, peu compatible avec les délais imposés par la procédure d’urgence- en mentionnant les hébergeurs via la référence aux personnes mentionnées au 2 du I de l’article 6 de la LCEN, le PLR présente une vulnérabilité majeure puisqu’il pourrait manquer les cibles spécifiées par Jean-Jacques Urvoas lors de sa conférence à l’ENSP.

Une solution partielle[59] à ce problème serait de considérer deux types d’hébergements physiques chez les hébergeurs, leur conférant ainsi un double statut juridique : un premier type ne relevant pas de la correspondance privée et relevant juridiquement de la définition du 2 du I de l’article 6 de la LCEN, d’une part. Et, d’autre part, les serveurs mails (ou tout serveur stockant des données relatives à une communication individuelle), qui feraient des hébergeurs -pour cette activité de stockage seulement- des opérateurs de communications électroniques, tels que mentionnés au L 34-1. Le fait de considérer un hébergeur faisant du stockage de mails non pas comme un hébergeur comme le remarquait Jean-Jacques Urvoas, mais comme un opérateur de communications, au sens de ‘personne morale fournissant au public un service de communications électroniques’[60] (catégorie la plus large, incluant aussi la radio et la télévision), permettrait donc le recueil de données relatives à des communications individuelles via des dispositifs temps réel installés chez les hébergeurs : en raison de ses conséquences sur les libertés civiles, cette interprétation pourrait donner lieu à des débats particuliers *si* la société civile s’empare de cette problématique en approfondissant les détails technico-juridiques du PLR, ce qui semble pour l’instant relativement peu probable.

Annexe 2 :

Données, informations, connaissances : la triple relativité de l'information dans la Société de l'information

«Frequently the messages have meaning; that is they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of communication are irrelevant to the engineering problem.»
Shannon [61]

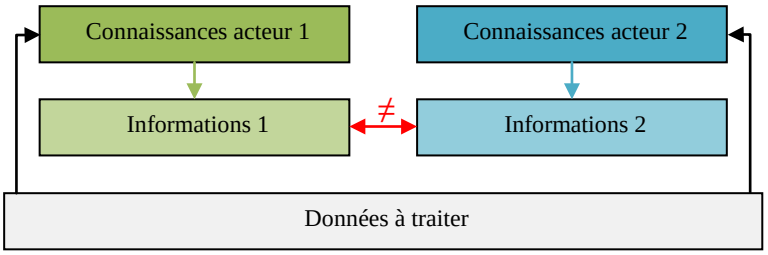
L'infocindynique s'intéresse aux aspects sémantiques et pragmatiques de l'information : à son sens, et à ses effets, en particulier téléologiques, donc comportementaux. La définition du mot 'information' retenue, faisant référence à l'aspect sémantique et n'ayant rien à voir avec les travaux de Shannon qui a clairement indiqué ne pas s'être intéressé aux aspects sémantiques, est la suivante : « *ce qu'il est possible d'extraire de données grâce à des connaissances*[62]»

Cette rédaction précise, ne spécifiant pas -à dessein- *quel* agent peut extraire de l'information, fait en fait référence à la description d'une triple relativité [63] de l'information, conçue précisément pour le contexte de la Société de l'information, et qu'il semble intéressant d'exposer dans le cadre de la discussion du PLR, puisque les notions de données, métadonnées et information y tiennent une place centrale.

Relativité horizontale

«Ein Epigramm, ob es wohl auch gut sei? Kannst du's entscheiden?
Weiß man doch eben nicht stets, was er sich dachte, der Schalk.»
Goethe[64]

Une première relativité est due aux différences de connaissances des acteurs traitant des données, et qui en extraient donc de ce fait des informations différentes :



Exemple : un constitutionnaliste et un architecte réseaux, disposant chacun de leurs connaissances spécifiques, ne tireront pas les mêmes informations du PLR (dont le texte constitue les données à traiter). Si les données à traiter sont par exemple celles d'un document technique relatif au modèle OSI, les constitutionnalistes auront sans doute plus de mal à en extraire des informations pertinentes. Ces dissonances peuvent être des facteurs de vulnérabilité : toute différence (ici épistémique) n'est pas forcément un facteur de vulnérabilité (et c'est d'ailleurs cette problématique, celle de la diversité, qui est à l'origine des Cindyniques du second ordre), mais en l'occurrence ces différences le sont pour les deux exemples précédents.

Un autre exemple intéressant est celui du choix graphique du Ministère de l'intérieur, qui avait disposé une main rouge sur le site de redirection des sites djihadistes dont il souhaite interdire l'accès. Pour certains internautes, cela n'évoque rien de sensible : ils n'y voient éventuellement qu'une référence au célèbre logo de l'association SOS Racisme et à la couleur d'un feu tricolore imposant un arrêt.

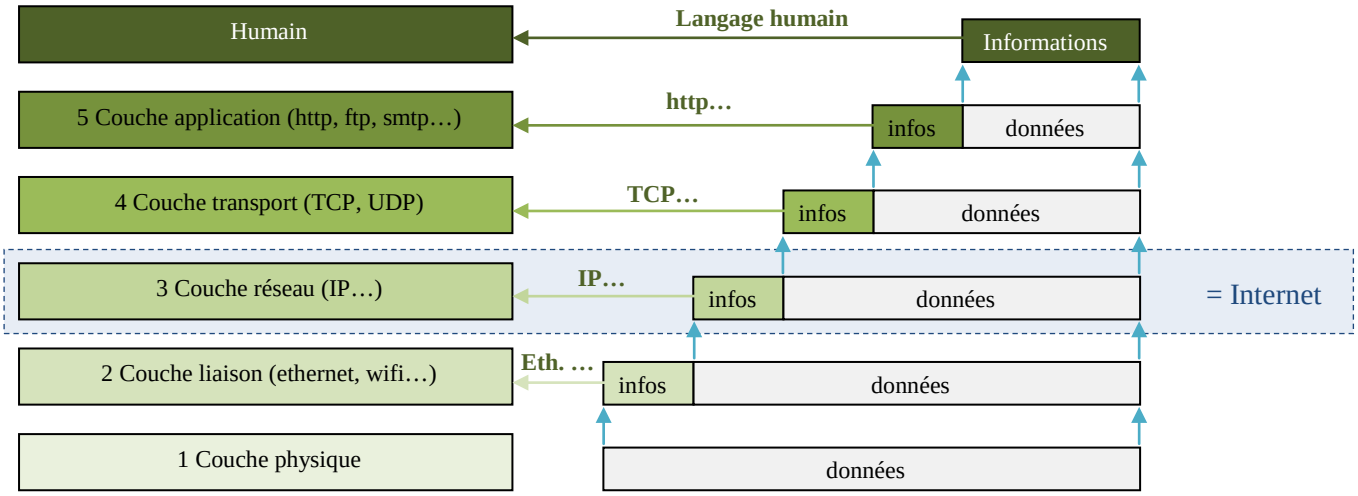
En revanche, pour des visiteurs férus de géopolitique méditerranéenne et d'histoire non officielle, ce choix graphique évoque immédiatement une manipulation massive du SDECE -désormais dévoilée- destinée à couvrir ses opérations de neutralisation, entre autres, de trafiquants d'armes. Il évoque aussi les exactions et attentats des 'barbouzes' du MPC[65], ravivant ainsi la question historique du terrorisme d'état[66], ce qui, dans le cadre de la prévention du terrorisme, n'est pas d'une géniale opportunité, en particulier en matière de soft power.

Enfin, cela évoque aussi directement l'affaire Farhat Ached, et, dès lors que certains acteurs *pourraient interpréter* ce choix graphique non comme une simple erreur de communication, mais comme une apologie intentionnelle, celui-ci heurte *de facto* frontalement les objectifs du Président de la République[67,68], qui avait il y a quelque temps transmis un dossier rassemblant l'ensemble des archives françaises disponibles relatives à cette affaire à la veuve de Fahrat Ached.

Relativité verticale

Une étude précédente consacrée à l'article 13 de la LPM suggérait[69] la nécessité de faire référence au modèle OSI lors de la rédaction des textes réglementant les activités du domaine des TIC. Ce sujet peut sembler un peu technique pour des juristes, fréquemment caractérisés par un déficit épistémique dans ce domaine, mais il est indispensable qu'ils en appréhendent au moins les éléments essentiels pour que les textes rédigés soient réellement compatibles avec l'esprit de la constitution :

Schématiquement, la Société de l'information repose sur la possibilité offerte aux hommes de communiquer entre eux via un réseau planétaire. Ce réseau, ou cet ensemble de réseaux, repose à la base sur une infrastructure physique : des câbles, des liaisons radio… Entre ce support physique et l'utilisateur humain, il y a un certain nombre de dispositifs organisé en « couches » empilées, par exemple la couche réseau qui permet le routage IP. Tout message échangé sur internet est découpé en paquets envoyés par un émetteur vers un destinataire, exactement comme une lettre envoyée par la poste : sur l'enveloppe le facteur peut lire l'adresse du destinataire et de l'émetteur, et à l'intérieur se trouve le message. Un routeur IP est l'équivalent d'un facteur lisant les adresses, ici écrites en 'langage' ou 'protocole' IP, pour transmettre les messages à bon port. Un routeur IP connaît le protocole IP et extrait donc les informations qui lui sont utiles des données se trouvant dans les en-têtes des paquets IP. En revanche, s'il est normalement constitué[70], il n'a pas connaissance du langage 'utilisé' par les données embarquées à l'intérieur du paquet, et ne peut donc pas en tirer d'informations.



Ces données embarquées sont transmises verticalement au dispositif de la couche supérieure (la couche 'transport') qui elle connaît des protocoles de couche 4, comme TCP, ou UDP. De la même façon, la couche 4 extrait les informations qui lui sont utiles des données TCP ou UDP, et transmet les données embarquées à une couche supérieure (la couche 'application'), qui elle connaît des protocoles comme http pour le web, smtp ou pop3 pour les mails, ou encore ftp pour les transfert de fichiers. Chaque application (web browser, client mail…) transmet enfin les données à l'utilisateur final, qui en tirera des informations grâce à ses propres connaissances humaines.

L'ensemble de ce système est donc organisé comme une pile de dispositifs fonctionnant sur un échange vertical de 'poupées russes', chaque couche étant capable de lire les informations de son niveau dans les données transmises : dans la Société de l'information, l'information extractible des données est *relative au niveau* de l'agent considéré, qui n'extrait de l'ensemble des données que les informations décodables grâce à la connaissance dont il dispose.

Une fois ce schéma appréhendé, le juriste peut par ailleurs réaliser à quel point les termes utilisés par le législateur sont imprécis au regard de la réalité des réseaux, qui nécessite plus de précisions que ce qui est nécessaire pour la téléphonie, ce qui le mène alors, entre autres, à ces questions :

Le L 34-1 exclut les données de 'contenu' que ce soit des correspondances, ou des informations consultées[71] :

► De quel contenu s'agit-il : de celui d'un mail ou d'une page web ? ou est-ce que l'adresse mail du destinataire ou l'URL de la page visitée sont aussi considérées comme des contenus?

► Comment comprendre le tarif WA09 de l'article A 43-9 du CPP qui suggère l'existence de fichiers IP/URL accessibles contre remboursement chez les opérateurs de communications électroniques?

En ce qui concerne les logs de connexion recueillis par les opérateurs de communications électroniques :

► Qu'est-ce qu'une 'communication' sur internet : Le fait de connecter un PC à une box ? le fait de recevoir un mail ou de consulter une page web? Une conversation Skype ou IRC?
► Qu'est-ce qu'un 'destinataire' d'une communication : L'adresse IP d'un serveur web ou smtp? l'adresse mail à laquelle un utilisateur écrit? Si le surf est une communication, l'URL d'une page visitée est-elle le destinataire de cette communication?

La référence à l'une ou l'autre de ces données peut radicalement changer la portée -l'ordre de grandeur- du dispositif, qui doit pourtant être connue si l'on veut pouvoir en évaluer la proportionnalité, actuellement inconnue du public.

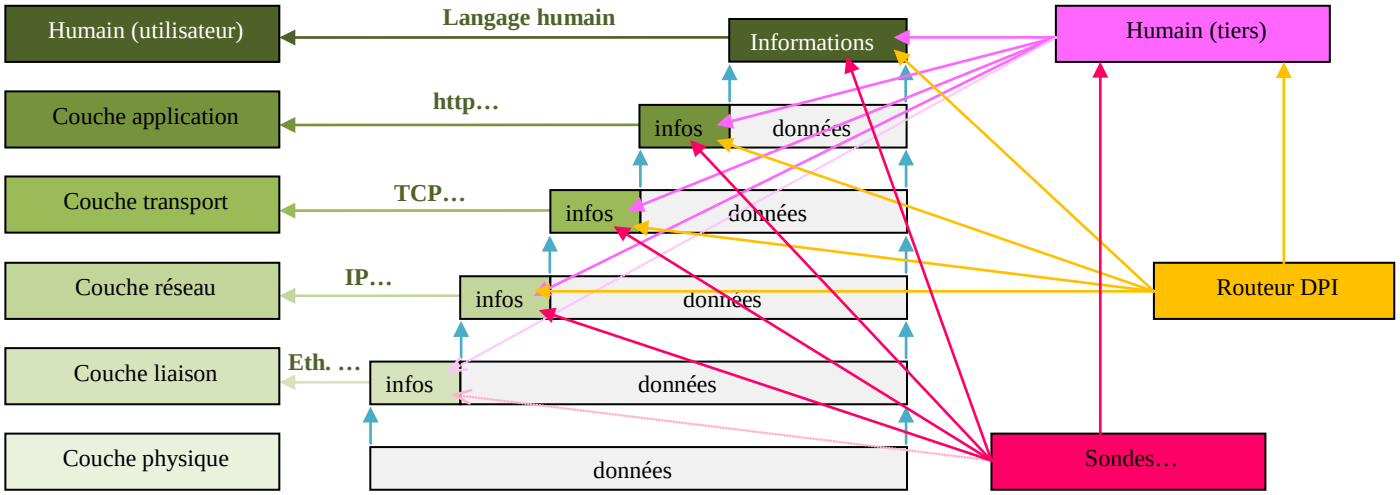
Relativité diagonale

«Je préfère que ce soit pas légal si vous voulez, voilà. »
Henri Guaino[72]

Un humain normal ne parle pas les protocoles réseaux et n'extrait donc pas d'informations des couches de données correspondantes. Cependant, il arrive que certains humains aient la capacité de comprendre ces protocoles et d'extraire des informations des données des couches correspondantes, et les exploitent par exemple à des fins de sécurité ou de surveillance.

De même, un routeur orthodoxe ne connaît que des protocoles de couche 3, mais certains acteurs promeuvent l'usage de routeurs DPI ('deep packet inspection') capables d'examiner les données embarquées dans les paquets IP et d'en extraire des informations grâce à leur connaissance des protocoles de couches supérieures, à des fins économiques, de sécurité ou de surveillance.

Enfin, s'agissant du PLR, une des questions importantes, au-delà de la définition juridique des acteurs atteignables, est la portée verticale des sondes et algorithmes, c'est-à-dire le périmètre des couches touchées par le recueil de données desquelles ils pourront extraire des informations à des fins d'exploitation, la même question valant d'ailleurs aussi pour les logs de connexion et les logs de contribution actuellement recueillis par les opérateurs et les hébergeurs.



Cette *capacité diagonale* de certains acteurs à extraire des informations de données des diverses couches du réseau est au cœur de la réflexion sur les métadonnées, cruciale en matière de libertés civiles. Le point important est que ces métadonnées ne sont pas des données pour ces acteurs, mais bien des *informations* décrivant les comportements individuels, bien éloignées des 'informations ou documents' de la loi de 91, qui n'étaient initialement que de simples données techniques nécessaires à la préparation d'une interception téléphonique extrajudiciaire.

Plus encore que les logs de connexion et de contribution, constituant à ce jour les 'informations ou documents', les dispositifs temps réel extrajudiciaires comme les sondes et algorithmes nécessitent -de par leur invasivité plus élevée- des références précises aux éléments réels du réseau si l'on veut pouvoir mesurer leur portée réelle et donc leur proportionnalité, notamment en vue de l'examen du texte par le conseil constitutionnel, souhaité par l'Elysée.

[1] RAPPORT FAIT AU NOM DE LA COMMISSION DES LOIS CONSTITUTIONNELLES, DE LA LÉGISLATION ET DE L'ADMINISTRATION GÉNÉRALE DE LA RÉPUBLIQUE, APRÈS ENGAGEMENT DE LA PROCÉDURE ACCÉLÉRÉE, SUR LE PROJET DE LOI (n° 2669) relatif au renseignement

[2] Délibération n° 2014-484 du 4 décembre 2014 portant avis sur un projet de décret relatif à l'accès administratif aux données de connexion et portant application de l'article L. 246-4 du code de la sécurité intérieure

[3] P. Cohet, Loi de Programmation Militaire 2014-2019 : Eléments d'évaluation du risque législatif lié à l'article 13. IFREI 2013.

[4] UN PROJET DE LOI POUR UNE SURVEILLANCE DE MASSE
Par ce projet de loi, la France autorise la surveillance de masse pour la prévention du terrorisme sans contrôle judiciaire ni recours effectif pour les victimes de surveillance.
Sans contrôle préalable judiciaire indépendant, le projet de loi légitime non seulement la mise en œuvre par les services de renseignement de techniques de surveillance ciblée mais aussi, dans le cas de la « prévention du terrorisme », la mise en œuvre de techniques de surveillance de masse, imposée à des opérateurs privés.
Toute surveillance doit être ciblée, fondée sur des soupçons plausibles et soumise à un contrôle judiciaire préalable. Ces mesures apparaissent ainsi comme illégales et disproportionnées et constituent une violation grave du droit au respect de la vie privée.
LES PRÉOCCUPATIONS SUR CE PROJET DE LOI
En amont des débats au Parlement prévus le 13 avril prochain, nous interpellons les députés sur les préoccupations suivantes :
- L'introduction de techniques illégales de surveillance de masse.
Dans le cas où le Premier ministre estimerait qu'une menace terroriste serait révélée, il pourrait alors, sans aucun contrôle, décider de la levée de l'anonymat de données collectées de façon automatique par les opérateurs.
- La création d'une présomption de surveillance légale.
Le projet de loi légalise des pratiques très intrusives de surveillance ciblée, en ne prévoyant qu'un contrôle juridictionnel a posteriori. La Commission nationale de contrôle des techniques de renseignement (CNCTR), nouvellement créée, n'a pas de réel pouvoir de contrainte ou d'interpellation.
- Les nouveaux champs d'intervention des renseignements définis de façon trop vague.
Le cadre d'intervention prévu par la loi pourrait ouvrir la voie à la mise en œuvre de mesures de surveillance contre une très large partie de la population.
- L'absence de recours effectif pour les victimes de surveillance illégitime devant le Conseil d'Etat.
La procédure est opaque et prévue à huit clos, ne permettant pas aux parties de se confronter.
http://www.amnesty.fr/Nos-campagnes/Liberte-expression/Actualites/Projet-de-loi-sur-le-renseignement-en-France-la-surveillance-de-masse-legalisee-14625

[5] Paris, le 17 mars 2015 — Les informations concernant le projet de loi sur le renseignement diffusées via Le Figaro aujourd'hui, avant sa présentation en Conseil des ministres jeudi 19 mars, confirment les inquiétudes déjà exprimées. Alors que la loi sur le renseignement était annoncée comme une grande loi permettant de protéger les droits fondamentaux, l'instrumentalisation sécuritaire des événements meurtriers de janvier risque d'aboutir à une incroyable dérive du gouvernement en matière de surveillance des citoyens. La Quadrature du Net appelle les citoyens et les députés à y résister.
Surveillance des comportements de tous les internautes par les intermédiaires techniques pour détecter les comportements suspects, accès en temps réel aux données de connexion, accès aux contenus des emails et enregistreurs de frappe au clavier, etc : l'éventail des mesures mises aux mains des services administratifs (police, douanes, etc.) sans contrôle du juge est d'une ampleur sans précédent.
Ne tirant aucune leçon des jurisprudences de la Cour de Justice de l'Union Européenne qui condamne la conservation trop longue et trop large des données personnelles des citoyens, le projet de loi envisage également une augmentation à 5 ans de la conservation des données par les services de renseignement.
Pour garantir les droits fondamentaux face à cet arsenal de mesures d'intrusion, de surveillance et de profilage, le gouvernement ne prévoit qu'une commission consultative, aux pouvoirs limités, ne permettant des recours qu'a posteriori et sans garanties réelles pour les citoyens.
En attendant le détail des mesures, La Quadrature du Net exhorte dès à présent les parlementaires à exercer leur devoir de contrôle, de raison et de défense des libertés publiques des citoyens face à ce projet de loi dangereux, et appelle les citoyens à se mobiliser.
Alors que les enquêtes, partout dans le monde, montrent que la surveillance de masse ne fait aucunement baisser le risque d'attentat, la voie prise par le gouvernement de Manuel Valls instaure une ère nouvelle de suspicion généralisée, marquant un recul historique de la séparation des pouvoirs et des droits fondamentaux. Si le Parlement acceptait de l'y suivre, les conditions d'un exercice correct de la démocratie ne seraient plus réunies.
https://www.laquadrature.net/fr/renseignement-desastreuse-derive-du-gouvernement-valls-sur-la-surveillance

[6] Présentant le projet de loi relatif au renseignement adopté en Conseil des ministres ce 19 mars 2015, le Premier ministre a fièrement assuré qu'il contenait « des moyens d'action légaux mais pas de moyens d'exception ni de surveillance généralisée des citoyens » !

Certes, ce projet légalise des procédés d'investigation jusqu'à présent occultes. Mais pour le reste, les assurances données quant au respect des libertés relèvent d'une rhétorique incantatoire et fallacieuse. Et, prétendant que ce projet de loi fait l'objet d'un large consensus, le gouvernement soumet l'examen du projet en procédure accélérée, confisquant ainsi le débat parlementaire.

« Pas de moyens d'exception » : sonoriser des espaces privés, capter des images, accéder en temps réel aux données de connexion Internet ou installer des dispositifs de recueil des communications couvrant de larges périmètres de l'espace public, suivant la technique du chalutier jetant son filet pour faire le tri ensuite : voilà donc des dispositifs qui ne constituent pas « des moyens d'exception » ! Faudrait-il donc admettre qu'ils relèveront dorénavant du quotidien le plus banal ?

« Pas de surveillance généralisée des citoyens » : au prétexte de la lutte légitime contre le terrorisme, le projet déborde largement hors de ce cadre. Il prévoit que les pouvoirs spéciaux de renseignement pourront être mis en œuvre pour assurer, notamment, « la prévention des violences collectives de nature à porter gravement atteinte à la paix publique ». Au nom de la lutte contre le terrorisme, ce sont donc aussi les mouvements de contestation sociale qui pourront faire l'objet de cette surveillance accrue. L'ensemble des citoyens constituera ainsi la cible potentielle du contrôle, à rebours de ce qui est affirmé.

Plus grave, tout le dispositif est placé entre les mains de l'exécutif évitant le contrôle par le juge judiciaire de mesures pourtant gravement attentatoires aux libertés individuelles qu'il est constitutionnellement chargé de protéger.

La vérification du respect des critères, particulièrement flous, de mise en œuvre de ces pouvoirs d'investigation exorbitants, est confiée à une commission qui fonctionne selon une logique inversée : pour les autoriser, un seul membre de la commission suffit, sauf en cas d'urgence, où l'on s'en passe. Mais pour recommander d'y renoncer, la majorité absolue des membres de la commission doit se prononcer, l'exécutif demeurant en dernier ressort libre d'autoriser la mesure. Et si la commission ne dit mot, elle consent. L'atteinte à la liberté devient ainsi la règle, la protection l'exception.

Ce n'est qu'a posteriori, et seulement si le filtre de la commission est passé, que des recours juridictionnels pourront être formés, exclusivement devant le Conseil d'Etat. Et, secret défense oblige, ils seront instruits sans respect du contradictoire. Ils resteront illusoires quoiqu'il en soit, puisque par définition, le plaignant doit être dans l'ignorance des mesures de surveillance qui peuvent le concerner.

Enfin, vice majeur du dispositif, aucune limite n'est fixée pour déterminer à quel moment et selon quels critères le régime du renseignement relevant d'une police administrative d'exception doit laisser place à une enquête judiciaire de droit commun, avec les garanties qu'elle comporte pour ceux qui en font l'objet. Le juge judiciaire pourrait donc continuer ainsi de rester à l'écart d'investigations portant sur des délits ou des crimes dont l'élucidation relève pourtant de sa mission.

Ce projet de loi installe un dispositif pérenne de contrôle occulte des citoyens dont il confie au pouvoir exécutif un usage quasi illimité. Il est à ce titre inacceptable. Seul un véritable contrôle a priori de techniques de renseignement proportionnées et visant un objectif strictement défini relevant de la sécurité nationale, restera respectueux des droits fondamentaux.

L'Observatoire des libertés et du numérique appelle les citoyens et les parlementaires à se mobiliser pour conduire ce projet vers sa seule finalité légitime : mettre les dispositifs d'encadrement de la surveillance et du renseignement en adéquation avec les exigences de l'Etat de droit.

Organisations membres de l'OLN : Cecil, Creis-Terminal, LDH, Quadrature du Net, Saf, SM.

http://www.syndicat-magistrature.org/Loi-renseignement-Tous-surveilles.html

[7] Paris, le 8 avril 2015. - L'Association des Services Internet Communautaires (ASIC), fondée en 2007 et qui regroupe l'ensemble des plates-formes d'hébergement Internet, françaises et internationales, s'inquiète de plusieurs dispositions prévues dans le projet de loi relatif au renseignement actuellement en cours de discussion à l'Assemblée nationale.

Alors que le Gouvernement n'a pas souhaité associer l'ASIC ou ses membres lors de l'élaboration du projet de loi, plusieurs membres de l'ASIC ont été invités individuellement au cycle d'auditions menées par le Président de la Commission des lois, Jean-Jacques Urvoas. Au cours de ces échanges, plusieurs points ont été soulevés – qui n'ont pas, pour l'heure fait l'objet des modifications nécessaires.

Comme avait eu l'occasion de le rappeler l'ASIC dès la publication du projet, toute mesure nouvelle de surveillance introduite par le projet de loi ne doit pas être redondante avec les nombreuses mesures déjà existantes, doit être proportionnée, transparente et soumise au contrôle d'une autorité dotée de pouvoirs et moyens suffisants.

Une loi qui "légalise" des pratiques existantes

D'une manière positive, le projet de texte renforce la transparence des mesures de surveillance mises en oeuvre, jusqu'alors de manière opaque et sans contrôle, par les services de renseignement.

A ce titre, il serait utile que le Gouvernement, notamment en amont des débats parlementaires, explicite le bilan de la mise en oeuvre des pratiques ainsi légalisées, notamment celles relatives aux boîtes noires déjà installées dans les réseaux des opérateurs de communication et leur impact sur la prévention d'actes de terrorisme sur le territoire.

Une loi qui instaure une surveillance généralisée pour identifier les cibles d'une surveillance plus fine.

Contrairement aux déclarations des membres du Gouvernement, l'ASIC considère que le projet de loi met en oeuvre des mesures aboutissant à l'instauration d'une surveillance généralisée.

En particulier, comme indiqué par le Gouvernement, les services de renseignement souhaiteraient installer des boîtes noires dans les infrastructures des diverses plates-formes d'hébergement de données, que ce soient des plates-formes de vidéos, des forums de discussion, des plates-formes de commerce électronique, des réseaux sociaux, etc., dans le but de collecter des informations.

Les débats sont venus préciser cette mesure : il s'agirait pour les autorités d'analyser en temps réel les données de tous les internautes visitant ces plates-formes afin d'identifier des comportements suspects.

Il s'agit bien d'une surveillance généralisée de tous les internautes, d'une analyse permanente du comportement de ces internautes

– afin d'identifier des comportements suspects qui feront l'objet ensuite d'enquêtes spécifiques.
Le plus étonnant est que les ministres rappellent que ces mesures visent à placer sous surveillance les "3000 personnes" qui représentent aujourd'hui une menace pour la sécurité nationale. Dès lors qu'un chiffre existe, cela signifie que ces personnes sont d'ores et déjà identifiées. En conséquence, le principe d'une collecte massive de données de tous les internautes apparaît disproportionnée.
Une loi qui délègue aux acteurs de l'Internet le soin de détecter les "individus suspects"
Avec les mécanismes de boîtes noires, les services de renseignement délèguent à des acteurs privés le soin de détecter les comportements suspects. En effet, et selon les précisions apportées lors des débats en Commission, il reviendrait alors aux acteurs du Web – sur la base de critères encore flous fournis par les autorités – de rechercher proactivement des individus potentiellement suspects.
Il ne s'agit pas de rechercher des personnes qui manifestement commettent ou s'apprêtent à commettre un crime ou un délit. Il s'agit bien de rechercher proactivement des personnes qui potentiellement pourraient représenter un danger pour la sécurité nationale.
En conséquence, et afin d'alléger la charge et la responsabilité forte qui pèseraient alors sur les acteurs privés, il ne fait pas de doute que le risque zéro s'appliquerait pour ces acteurs privés : application large des critères avec une remontée massive d'informations auprès des autorités.
"En faisant peser sur les entreprises privées le soin de détecter les comportements suspects et donc la responsabilité en cas d'échec, le Gouvernement va instituer de facto une véritable "course à la délation" de la part des acteurs de l'internet", ont tenu à préciser les dirigeants de l'ASIC.
Des boîtes noires qui vont collecter non plus des données techniques, mais toute la vie des internautes
Alors que le texte demeurait silencieux sur ce point, le Gouvernement est venu expliciter la teneur des données auquel il souhaitait avoir accès par l'intermédiaire de ces boîtes noires.
A l'occasion des débats au sein de la Commission des Lois, le Ministre de l'intérieur a indiqué que les algorithmes contenus dans les boîtes noires devraient permettre, au travers de l'analyse des profils des internautes, d'identifier les comportements suspects.
La loi distingue aujourd'hui entre deux types d'accès : l'accès aux données purement techniques (par exemple, les adresses IP des personnes ayant mis en ligne une vidéo) et les données de contenus (par exemple, les emails ou les adresses des sites internet visités par un internaute). Si la première catégorie est accessible sur la base d'une simple réquisition ou requête administrative, la deuxième catégorie de données fait l'objet d'un encadrement très strict: accès limité dans le temps, ciblage sur une ou plusieurs personnes pré-identifiées, contrôle judiciaire.
Ici, le Gouvernement cherche à s'affranchir de l'ensemble de ces contraintes. En voulant utiliser des boites noires pour "profiler" les internautes français, les services de renseignement cherchent de facto à récolter l'ensemble des données de contenus dont les internautes peuvent être à l'origine (par exemple, cercle d'amis dans un réseau social, historique des sites visités, etc.).
"Le mécanisme de boîtes noires cherchent à mettre en oeuvre une collecte systématique de l'ensemble des internautes, de l'ensemble des contenus qu'ils visitent ou qu'ils regardent et cela en s'affranchissant totalement des garde-fous existants" ont précisé les membres de l'ASIC.
Pour se dédouaner, le Gouvernement tente d'expliquer que des pratiques comparables seraient déjà mises en oeuvre par les acteurs privés à des fins commerciales. Mais, il oublie de préciser que de nombreux garde-fous existent à savoir:

un contrôle, voire des sanctions, de la part des diverses autorités de protection des données en Europe ;
une information préalable et un recueil du consentement de la part des internautes ;
et la possibilité offerte aux internautes de pouvoir contrôler leurs données – à savoir en supprimer, en modifier le contenu voire les exporter pour les porter vers d'autres services.

Or, il semble que ces garde-fous n'aient pas été prévus par le projet de loi. "Si le Gouvernement souhaite ainsi comparer les pratiques, il se doit alors de placer ces pratiques des services de renseignement sous un contrôle complet de la part de la CNIL, d'informer les individus qui en sont l'objet et enfin, leur permettre de modifier, supprimer ou exporter, les données ainsi collectées", ont tenu à rappeler les membres de l'ASIC.
Ainsi, en collectant et en agrégeant toutes les données, émanant de divers sites internet (réseaux sociaux, plates-formes vidéos, etc.), les services de renseignement seront en mesure de tout connaître sur chaque individu.
En conséquence, l'ASIC appelle de ses voeux à la suppression pure et simple de ce dispositif permettant l'installation de boîtes noires dans les infrastructures d'intermédiaires techniques.
A défaut, outre la mise en oeuvre d'une surveillance sans précédent en France, de telles mesures risquent de remettre en cause l'attractivité de la France pour les acteurs du numérique, par exemple, les exploitants d'infrastructure (data center, points d'interconnexion, câbles sous-marins) qui feront tout pour éviter notre territoire. La France poursuivra alors sa lente descente dans la récession numérique.
http://www.lasic.fr/?p=732

[8] Communiqué de la CGT Paris.
Les attentats terroristes de janvier 2015 ont exacerbé le sentiment de peur dans notre pays. Le pouvoir en place a utilisé ce sentiment pour proposer une loi qui, sous couvert de lutte contre le terrorisme, est certainement la plus liberticide qui soit. Jamais une loi aussi privative de liberté n'aura été proposée, sauf pendant la guerre d'Algérie.
A l'époque cette loi « confère aux autorités civiles, dans l'aire géographique à laquelle elle s'applique, des pouvoirs de police exceptionnels portant sur la réglementation de la circulation et du séjour des personnes, sur la fermeture des lieux ouverts au public et sur la réquisition des armes ». Cette loi est d'ailleurs toujours en vigueur et a été utilisée lors des « émeutes de banlieue » en 2005.

Ainsi, un gouvernement qui se prétend de gauche n'hésite pas à continuer d' instrumentaliser ceux qui sont morts pour la liberté d'expression, ou en raison de leur religion, pour faire passer une loi qui ne va pas seulement concerner le terrorisme, la prolifération d'armes de destruction massive ou encore la contre-ingérence, mais qui va se glisser dans des domaines plus variés tels que les "intérêts majeurs de politique étrangère" et les "violences collectives pouvant porter gravement atteinte à la paix publique".
Que viennent faire ces deux notions dans la lutte contre le terrorisme ? Quel rapport ont-elles avec la mort de journalistes, de personnes en raison de leur religion ?
Qui va définir la nature de ces "intérêts majeurs" ou décider de ce qu'on doit considérer comme "violences collectives" ? Une simple manifestation ne pourrait- elle pas être classée dans cette catégorie ?
Ainsi, toute personne participant à un rassemblement pourrait être mise sur écoute ? Que devient alors le droit au respect de la vie privée ?
Sans parler du flou juridique total qui entoure les outils qui seront ainsi à disposition des services de renseignements.
Cette loi est une atteinte grave aux libertés fondamentales dans notre pays.
La CGT Paris comprend qu'il est nécessaire de lutter activement contre toute forme de terrorisme, mais cela ne doit pas se faire au détriment des libertés publiques et de la démocratie !
Cette loi est d'autant plus dangereuse qu'elle donne tous les pouvoirs à une seule personne. En effet ce serait le Premier ministre, qui déciderait qui doit être surveillé ou non. Et on s'étonne que l'opposition annonce qu'elle va voter cette loi !
De l'avis même de Marc TREVIDIC, juge spécialisé dans le terrorisme, il s'agit de donner des pouvoirs exorbitants aux services de renseignements dans des domaines biens plus larges que la seule lutte contre le terrorisme, parlant de notions particulièrement vagues. Il précise que : "Ces pouvoirs exorbitants se feront sans contrôle judiciaire". Ne mentons pas aux Français en présentant ce projet comme une loi antiterroriste. Il ouvre la voie à la généralisation de méthodes intrusives, hors du contrôle des juges judiciaires, pourtant garants des libertés individuelles ».
La CGT Paris exige le retrait de ce projet de loi liberticide qui se veut un « patriot act » à la française et remet gravement en cause le principe de la liberté d'expression, individuelle et collective, dans notre pays.
Ce sont bien les politiques menées par Hollande, Valls et consorts qui forment le creuset de la violence, du terrorisme, en divisant, en opposant les salariés entre eux, en détricotant toutes les garanties collectives, en cassant l'emploi public les services publics, en se soumettant aux institutions financières, aux banques et au grand patronat…
http://www.humanite.fr/projet-de-loi-sur-le-renseignement-un-texte-liberticide-cgt-570511

[9] Projet de loi sur le renseignement : La liberté d'être surveillé et de ne plus manifester !

La peur... la peur est un outil incroyablement puissant. Les récents attentats terroristes ont exacerbé ce sentiment, donnant ainsi la possibilité à nos gouvernants de proposer une loi qui, sous couvert de mieux protéger contre le terrorisme, va en réalité être une des plus liberticides jamais votées depuis celle sur l'état d'urgence.
Utilisant ainsi les gens qui sont morts pour la liberté d'expression, ou en raison de leur religion, un gouvernement de gauche (!) veut faire passer une loi qui ne va pas seulement concerner le terrorisme, la prolifération d'armes de destruction massive ou encore la contre-ingérence, mais qui va se glisser dans des domaines plus variés tels que les "intérêts majeurs de politique étrangère" et les "violences collectives pouvant porter gravement atteinte à la paix publique".
Que viennent faire ces deux catégories dans la lutte contre le terrorisme ? Quel rapport ont-elles avec la mort de journalistes, de personnes en raison de leur religion ou de nos collègues ?
Qui va définir la nature de ces "intérêts majeurs" ou décider de ce qu'on doit considérer comme "violences collectives" ? Une simple manifestation ne pourrait elle pas être classée dans cette catégorie, vu le "risque" inhérent de ce genre de rassemblement qu'il tourne mal ?
Toute personne participant à un rassemblement pourrait être mise sur écoute ? Réalisez-vous ce que ça implique quant au respect de la vie privée ?!
Sans parler du flou juridique total qui entoure les outils qui seront ainsi à disposition des services de renseignements.
La CGT-POLICE comprend qu'il soit nécessaire de lutter activement contre toute forme de terrorisme, mais cela ne doit pas se faire au prix des libertés publiques !
Car c'est ce que cette loi est : une atteinte grave à ces libertés !
Et tout cela dans les mains d'une seule personne : le Premier ministre, qui décidera qui doit être surveillé ou non. Et on s'étonne que l'opposition annonce qu'elle va voter cette loi !
De l'avis même de Marc TREVIDIC, juge spécialisé dans le terrorisme, il s'agit de donner des pouvoirs exorbitants aux services de renseignements dans des domaines biens plus larges que la seule lutte contre le terrorisme, parlant de notions particulièrement vagues. Il précise que : "Ces pouvoirs exorbitants se feront sans contrôle judiciaire". Ne mentons pas aux Français en présentant ce projet comme une loi antiterroriste. Il ouvre la voie à la généralisation de méthodes intrusives, hors du contrôle des juges judiciaires, pourtant garants des libertés individuelles dans notre pays."
La CGT-POLICE, en mémoire notamment de nos collègues tombés pour protéger une liberté individuelle qu'est la "liberté d'expression", demande l'abandon de cette loi telle qu'elle a été présentée et en demande une nouvelle non seulement recentrée sur le terrorisme, mais dotée de garde-fous beaucoup plus importants qu'une simple commission administrative qui serait, comme à l'accoutumée, privée des moyens et personnels nécessaires à la mise en œuvre de sa mission de surveillance.
http://cgtpolice75.fr/spip.php?article107

[10] http://www.lexpress.fr/actualite/projet-de-loi-sur-le-renseignement-les-reserves-du-juge-antiterroriste-marc-trevidic_1662838.html

[11] http://www.cnnumerique.fr/renseignement/

[12] http://www.aef.info/depeche/libre/498047

[13] http://www.lebardegandi.net/post/2015/04/03/Projet-de-loi-sur-le-renseignement

[14] http://www.lemonde.fr/pixels/article/2015/04/10/loi-sur-le-renseignement-des-hebergeurs-de-donnees-menacent-de-delocaliser_4613333_4408996.html

[15] http://moreas.blog.lemonde.fr/2015/04/12/loi-sur-le-renseignement-les-petits-les-gros-les-bons-et-les-mechants/#more-7909

[16] Commission de la défense nationale et des forces armées, Mardi 24 mars 2015 Séance de 18 heures 30, Compte rendu n° 48.

[17] P. Cohet, Loi de Programmation Militaire 2014-2019 : Eléments d'évaluation du risque législatif lié à l'article 13. IFREI 2013.

[18] Exemple de l'avis de la CNIL, dans sa Délibération n° 2014-484 du 4 décembre 2014 portant avis sur un projet de décret relatif à l'accès administratif aux données de connexion et portant application de l'article L. 246-4 du code de la sécurité intérieure (demande d'avis n° AV 14027710) :
« Sur les réquisitions prévues à l'article L. 246-3 du CSI
L'article R. 246-7 du CSI, tel que prévu par le projet de décret, se rapporte aux demandes d'informations et de documents prévues à l'article L. 246-3 du CSI, lequel se réfère à la notion de « sollicitation du réseau » et de transmission en temps réel.
La commission rappelle que ce nouveau type de réquisition bénéficie de garanties particulières par rapport aux réquisitions classiques de données de connexion, puisque, notamment à sa demande, il lui a été appliqué un régime proche de celui applicable aux interceptions de sécurité (contrôle a priori du Premier ministre et a posteriori de la CNCIS).
Ces demandes de recueil d'informations ou de documents en application de l'article L. 246-3 du CSI devront comporter leur motivation au regard des finalités mentionnées à l'article L. 241-2 du CSI et la nature des informations ou documents dont le recueil est demandé, ainsi que la durée de ce recueil. Les données à caractère personnel relatives à l'agent et à l'origine de la demande ne figurent pas au titre des éléments définissant cette demande. Si de telles données étaient nécessaires à ce type de réquisition, la commission invite le SGDSN à modifier le projet de décret en ce sens. Enfin, et à l'identique des réquisitions mentionnées à l'article L. 246-1 du CSI, la motivation de la demande n'est pas communiquée aux opérateurs.
Concernant le périmètre de ce nouveau type de réquisition, si les précisions apportées par les débats parlementaires incitaient à penser que cette disposition se limitait exclusivement à l'utilisation de la géolocalisation, le SGDSN a toutefois infirmé cette position en indiquant qu'il convenait que les dispositions réglementaires ne soient pas figées dans le temps au regard des évolutions technologiques. Au regard des risques potentiels en matière de protection de la vie privée et de protection des données personnelles, la commission ne peut que regretter que le projet de décret ne permette pas de définir précisément et limitativement le périmètre de ce nouveau type de réquisition. »

[19] « La section 3 du chapitre II du titre Ier du livre II de la partie réglementaire (Décrets en Conseil d'Etat) du code des postes et des communications électroniques intitulée : « Protection de la vie privée des utilisateurs de réseaux et services de communications électroniques » comprend les articles R. 10-12, R. 10-13 et R. 10-14 ainsi rédigés :
« Art. R. 10-12. - Pour l'application des II et III de l'article L. 34-1, les données relatives au trafic s'entendent des informations rendues disponibles par les procédés de communication électronique, susceptibles d'être enregistrées par l'opérateur à l'occasion des communications électroniques dont il assure la transmission et qui sont pertinentes au regard des finalités poursuivies par la loi.
« Art. R. 10-13. - I. - En application du II de l'article L. 34-1 les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales :
« a) Les informations permettant d'identifier l'utilisateur ;
« b) Les données relatives aux équipements terminaux de communication utilisés ;
« c) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;
« d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;
« e) Les données permettant d'identifier le ou les destinataires de la communication.
« II. - Pour les activités de téléphonie l'opérateur conserve les données mentionnées au I et, en outre, celles permettant d'identifier l'origine et la localisation de la communication.
« III. - La durée de conservation des données mentionnées au présent article est d'un an à compter du jour de l'enregistrement.
« IV. - Les surcoûts identifiables et spécifiques supportés par les opérateurs requis par les autorités judiciaires pour la fourniture des données relevant des catégories mentionnées au présent article sont compensés selon les modalités prévues à l'article R. 213-1 du code de procédure pénale.

« Art. R. 10-14. - I. - En application du III de l'article L. 34-1 les opérateurs de communications électroniques sont autorisés à conserver pour les besoins de leurs opérations de facturation et de paiement les données à caractère technique permettant d'identifier l'utilisateur ainsi que celles mentionnées aux b, c et d du I de l'article R. 10-13.
« II. - Pour les activités de téléphonie, les opérateurs peuvent conserver, outre les données mentionnées au I, les données à caractère technique relatives à la localisation de la communication, à l'identification du ou des destinataires de la communication et les données permettant d'établir la facturation.
« III. - Les données mentionnées aux I et II du présent article ne peuvent être conservées que si elles sont nécessaires à la facturation et au paiement des services rendus. Leur conservation devra se limiter au temps strictement nécessaire à cette finalité sans excéder un an.
« IV. - Pour la sécurité des réseaux et des installations, les opérateurs peuvent conserver pour une durée n'excédant pas trois mois :
« a) Les données permettant d'identifier l'origine de la communication ;
« b) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;
« c) Les données à caractère technique permettant d'identifier le ou les destinataires de la communication ;
« d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs. »
» Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques

[20] «Les données mentionnées au II de l'article 6 de la loi du 21 juin 2004 susvisée, que les personnes sont tenues de conserver en vertu de cette disposition, sont les suivantes :
1° Pour les personnes mentionnées au 1 du I du même article et pour chaque connexion de leurs abonnés :
a) L'identifiant de la connexion ;
b) L'identifiant attribué par ces personnes à l'abonné ;
c) L'identifiant du terminal utilisé pour la connexion lorsqu'elles y ont accès ;
d) Les dates et heure de début et de fin de la connexion ;
e) Les caractéristiques de la ligne de l'abonné ;
2° Pour les personnes mentionnées au 2 du I du même article et pour chaque opération de création :
a) L'identifiant de la connexion à l'origine de la communication ;
b) L'identifiant attribué par le système d'information au contenu, objet de l'opération ;
c) Les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus ;
d) La nature de l'opération ;
e) Les date et heure de l'opération ;
f) L'identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a fourni ;
3° Pour les personnes mentionnées aux 1 et 2 du I du même article, les informations fournies lors de la souscription d'un contrat par un utilisateur ou lors de la création d'un compte :
a) Au moment de la création du compte, l'identifiant de cette connexion ;
b) Les nom et prénom ou la raison sociale ;
c) Les adresses postales associées ;
d) Les pseudonymes utilisés ;
e) Les adresses de courrier électronique ou de compte associées ;
f) Les numéros de téléphone ;
g) Le mot de passe ainsi que les données permettant de le vérifier ou de le modifier, dans leur dernière version mise à jour ;
4° Pour les personnes mentionnées aux 1 et 2 du I du même article, lorsque la souscription du contrat ou du compte est payante, les informations suivantes relatives au paiement, pour chaque opération de paiement :
a) Le type de paiement utilisé ;
b) La référence du paiement ;
c) Le montant ;
d) La date et l'heure de la transaction.
Les données mentionnées aux 3° et 4° ne doivent être conservées que dans la mesure où les personnes les collectent habituellement.»
Décret n° 2011-219 du 25 février 2011 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

[21] Voire 11 ans en se référent au 43-9 issu de l'article 1 de la loi du 1er août 2000, dont le décret d'application n'a jamais été publié avant son abrogation. http://www.senat.fr/application-des-lois/audiovisuel.html

[22] Cf. l'ARCEP : Avis n° 2013-0952 du 23 juillet 2013 sur les projets d'arrêtés relatifs à la tarification des réquisitions judiciaires, des interceptions de sécurité et la fourniture des données par les opérateurs de communications électroniques

« En effet, bien que les articles L. 34-1-1 et R. 10-13 du code des postes et des communications électroniques imposent aux opérateurs la conservation de ces données, les tarifs des prestations dédiées à l'internet n'avaient encore jamais été fixés. Il s'agit de sept prestations dans le cadre des enquêtes judiciaires et de six prestations dans le cadre de la lutte contre le terrorisme. La détermination et la tarification de ces prestations permettent ainsi aux opérateurs de connaître de manière précise et transparente les données qu'ils sont susceptibles de devoir fournir ainsi que les tarifs associés. »

[23] « Une première ambigüité dûe à l'abrogation du L 34-1-1 et du II bis concernait en particulier la nature des données jusque-là limitées par le L 34-1-1 et le décret du II/II bis. Fleur Pellerin ayant évoqué[23] la possibilité d'un décret précis, une autre ambigüité est apparue, certains acteurs ayant remarqué que le seul décret prévu par l'article 20 (au L 246-4) ne semblait pas *a priori* destiné à porter de telles précisions, sans doute nécessaires au regard de l'article 8 de la CEDH.

Face aux oppositions exprimées la Direction de la législation et du contrôle du Sénat a publié un communiqué de presse par lequel Jean-Louis Carrère, Président de la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat et rapporteur du texte, a clarifié l'intention du législateur[23] : Les données de connexion sont celles prévues par le L43-1, et les données d'identification celles prévues par le II de l'article 6 de la LCEN. Deux décrets précisent respectivement ces données : 2006-358, et 2011-219. »

P. Cohet, Loi de Programmation Militaire 2014-2019 : Eléments d'évaluation du risque législatif lié à l'article 13. IFREI 2013.

[24] « Ce nouveau dispositif ne modifie aucunement ni la nature des données concernées ni la procédure permettant aux services de renseignement d'avoir accès à ces données.

Il permettra de recueillir les données de connexion conservées par les opérateurs de communications électroniques et par les hébergeurs de contenus. Les premiers sont tenus de conserver ces données en application de l'article L. 34-1 du code des postes et communications électroniques, les seconds sont tenus de les conserver en application de l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique. Si la rédaction de l'article 13 fait référence aux « informations ou documents » « traités ou conservés », elle ne fait que reprendre la rédaction actuelle de l'article L. 244-2 du code de la sécurité intérieure.

Ainsi, aucune extension du champ des données accessibles par rapport au droit existant n'est prévue. L'accès aux contenus des communications reste du ressort exclusif du régime des interceptions de sécurité, qui demeure totalement inchangé. »

(Communiqué de presse mentionné à la note précédente)

[25] « Art. R. 246-1.-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. 10-13 et R. 10-14 du code des postes et des communications électroniques et à l'article 1er 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.

Décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion

[26] Guisnel, Jean; Korn-Brzoza, David (2014-09-25). Au service secret de la France: Les maîtres de l'espionnage se livrent enfin... Martinière Beaux-livres(De La). Kindle Edition.

[27] Article L241-2

« Peuvent être autorisées, à titre exceptionnel, dans les conditions prévues par l'article L. 242-1, les interceptions de correspondances émises par la voie des communications électroniques ayant pour objet de rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de l'article L. 212-1. »

[28] http://www.assemblee-nationale.fr/14/projets/pl2669-ei.asp#P1356_217226

[29] Déplacé dans le 851-5 par la Commission des lois

http://www.assemblee-nationale.fr/14/amendements/2669/CION_LOIS/CL179.asp

Article 2

I. – Le livre VIII du code de la sécurité intérieure, tel qu'il résulte de l'article 1er de la présente loi, est complété par un titre V intitulé : « Des techniques de recueil du renseignement soumises à autorisation ».

II. – Au même titre V, il est inséré un chapitre Ier intitulé « Des accès administratifs aux données de connexion » et comprenant les articles L. 851-1 à L. 851-10, tels qu'ils résultent du II *bis* du présent article.

II *bis*. – Le même code est ainsi modifié :

1° L'article L. 246-1 devient l'article L. 851-1 et est ainsi modifié :

a) La référence : « L. 241-2 » est remplacée par la référence : « L. 811-3 » ;

b) (nouveau) Sont ajoutés deux alinéas ainsi rédigés :

« Pour les finalités mentionnées à l'article L. 811-3 et par dérogation à l'article L. 821-2, les demandes motivées des agents individuellement désignés et dûment habilités des services spécialisés de renseignement sont transmises directement à la Commission nationale de contrôle des techniques du renseignement qui rend son avis dans les conditions prévues à l'article L. 821-3.

« Un service du Premier ministre est chargé de recueillir les informations ou documents auprès des opérateurs et des personnes mentionnés au premier alinéa du présent article. » ;

2° L'article L. 246-2 est abrogé ;

3° Après l'article L. 851-1, tel qu'il résulte du 1° du présent II *bis*, sont insérés des articles L. 851-2 à L. 851-4 ainsi rédigés :

« *Art. L. 851-2. – (Supprimé)*

« *Art. L. 851-3*. – Pour les seuls besoins de la prévention du terrorisme, peut être autorisé le recueil des informations et des documents mentionnés à l'article L. 851-1 relatifs à des personnes préalablement identifiées comme présentant une menace opéré en temps réel sur les réseaux des opérateurs et des personnes mentionnés au même article L. 851-1.

« Ces dispositions sont mises en œuvre sous le contrôle du Premier ministre, après avis de la Commission nationale de contrôle des techniques de renseignement, dans les conditions prévues au chapitre I[er] du titre II du présent livre.

« *Art. L. 851-4*. – Pour les seuls besoins de la prévention du terrorisme, le Premier ministre ou l'une des personnes déléguées par lui peut, après avis de la Commission nationale de contrôle des techniques de renseignement, imposer aux opérateurs et aux personnes mentionnés à l'article L. 851-1 la mise en œuvre sur leurs réseaux d'un dispositif destiné à détecter une menace terroriste sur la base de traitements automatisés des seules informations ou documents mentionnés au même article L. 851-1, sans procéder à l'identification des personnes auxquelles ces informations ou documents se rapportent et sans procéder au recueil d'autres données que celles qui répondent aux critères de conception des traitements automatisés.

« Si une telle menace est ainsi révélée, le Premier ministre ou l'une des personnes déléguées par lui peut décider, après avis de la Commission nationale de contrôle des techniques de renseignement dans les conditions prévues au chapitre I[er] du titre II du présent livre, de procéder à l'identification des personnes concernées et au recueil des informations ou documents afférents. Leur exploitation s'effectue alors dans les conditions prévues au chapitre II du même titre.

« La Commission nationale de contrôle des techniques de renseignement émet un avis sur le dispositif et les critères des traitements automatisés mentionnés au premier alinéa du présent article. Elle dispose d'un accès permanent à ceux-ci, est informée de toute modification apportée et peut émettre des recommandations. Lorsqu'elle estime que les suites données à ses avis ou à ses recommandations sont insuffisantes, elle peut faire application de l'article L. 821-6. » ;

4° L'article L. 246-3 devient l'article L. 851-5 et est ainsi modifié :

a) Le premier alinéa est ainsi modifié :

– la référence : « L. 241-2 » est remplacée par la référence : « L. 811-3 » ;

– la référence : « L. 246-1 » est remplacée par la référence : « L. 851-1 » ;

– à la fin, les mots : « aux agents mentionnés au I de l'article L. 246-2 » sont remplacés par les mots : « à un service du Premier ministre » ;

Les quatre derniers alinéas sont remplacés par deux alinéas ainsi rédigés :

« Le recueil des informations ou documents mentionnés à l'article L. 851-1 peut également être autorisé au moyen d'un appareil ou d'un dispositif technique mentionné au 1° de l'article 226-3 du code pénal, qui fait l'objet d'une inscription dans un registre spécial tenu à la disposition de la Commission de contrôle des techniques de renseignement et qui ne peut être mis en œuvre que par des agents individuellement désignés et dûment habilités. Un service du Premier ministre centralise les informations ou documents recueillis, qui sont détruits dès qu'il apparaît qu'ils ne sont pas en rapport avec l'autorisation de mise en œuvre, dans un délai maximal de trente jours.

« L'autorisation de recueil de ces informations ou documents, mentionnée au présent article, est accordée dans les conditions prévues au chapitre I[er] du titre II du présent livre. Elle peut être renouvelée dans les mêmes conditions de forme et de durée. » ;

5° Après l'article L. 851-5, tel qu'il résulte du 4°, sont insérés des articles L. 851-6 et L. 851-7 ainsi rédigés :

« *Art. L. 851-6.* – Pour les finalités mentionnées à l'article L. 811-3, peut être autorisée l'utilisation d'un dispositif technique permettant la localisation en temps réel d'une personne, d'un véhicule ou d'un objet.

« *Art. L. 851-7. – (Supprimé)* » ;

6° L'article L. 246-5 devient l'article L. 851-8 et la référence : « L. 246-1 » est remplacée par la référence : « L. 851-1 » ;

7° Le second alinéa de l'article L. 246-4 devient l'article L. 851-9 et le mot : « article » est remplacé par le mot : « chapitre » ;

8° *(nouveau)* Après l'article L. 851-9, tel qu'il résulte du 7° du présent II *bis*, il est inséré un article L. 851-10 ainsi rédigé :

…http://www.assemblee-nationale.fr/14/ta-commission/r2697-a0.asp

[30] http://www.cnil.fr/linstitution/actualite/article/article/publication-de-lavis-sur-le-projet-de-loi-relatif-au-renseignement/

[31] Guisnel, Jean; Korn-Brzoza, David (2014-09-25). Au service secret de la France: Les maîtres de l'espionnage se livrent enfin... Martinière Beaux-livres(De La). Kindle Edition.

[32] Intervention radio de Tristan Nitot : « *ce qui m'a frappé dans ce projet de loi c'est la mise en place de la surveillance de masse sur internet et ça c'est la ligne jaune qui à mon sens ne doit pas être franchie* »
http://radionotredame.net/player/http://radionotredame.net/wp-content/uploads/podcasts/le-debat-du-soir/le-debat-du-soir-24-03-2015.mp3

[33] http://www.aef.info/depeche/libre/498047

[34] http://www.assemblee-nationale.fr/14/pdf/rapports/r2697.pdf

[35] Article 29

I. - Après l'article L. 32-3 du code des postes et télécommunications, sont insérés deux articles L. 32-3-1 et L. 32-3-2 ainsi rédigés : « Art. L. 32-3-1. - I. - Les opérateurs de télécommunications, et notamment ceux mentionnés à l'article 43-7 de la loi no 86-1067 du 30 septembre 1986 précitée, sont tenus d'effacer ou de rendre anonyme toute donnée relative à une communication dès que celle-ci est achevée, sous réserve des dispositions des II, III et IV.

« II. - Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire d'informations, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le IV, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'Etat, par les opérateurs.

« III. - Pour les besoins de la facturation et du paiement des prestations de télécommunications, les opérateurs peuvent, jusqu'à la fin de la période au cours de laquelle la facture peut être également contestée ou des poursuites engagées pour en obtenir le paiement, utiliser, conserver et, le cas échéant, transmettre à des tiers concernés directement par la facturation ou le recouvrement les catégories de données techniques qui sont déterminées, dans les limites fixées par le IV, selon l'activité des opérateurs et la nature de la communication, par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés.

« Les opérateurs peuvent en outre réaliser un traitement de ces données en vue de commercialiser leurs propres services de télécommunications, si les usagers y consentent expressément et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période correspondant aux relations contractuelles entre l'usager et l'opérateur.

« IV. - Les données conservées et traitées dans les conditions définies aux II et III portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs et sur les caractéristiques techniques des communications assurées par ces derniers.

« Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications.

« La conservation et le traitement de ces données s'effectuent dans le respect des dispositions de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

« Les opérateurs prennent toutes mesures pour empêcher une utilisation de ces données à des fins autres que celles prévues au présent article.

http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=75FDDB1256EF96ACDB1703C292FBA694.tpdila11v_1?cidTexte=JORFTEXT000000222052&categorieLien=id

[36] "*La Commission a adopté un amendement du rapporteur pérennisant les dispositions précitées des articles 29, 30 et 31 de la loi du 15 novembre 2001 (amendement n° 86).*"
http://www.assemblee-nationale.fr/12/rapports/r0508.asp

[37] Loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000439399

[38] "*Article 4*

Le I de l'article L. 34-1 du code des postes et des communications électroniques est complété par l'alinéa suivant : « Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article. »"

[39] Article 1

Le chapitre Ier du titre II du livre III de la partie 2 de la partie réglementaire du code de la défense est ainsi rédigé :

« Chapitre Ier
« Responsabilités
« Section 1
« Autorité nationale de sécurité des systèmes d'information
« Art. R. 2321-1.-L'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 est l'Agence nationale de la sécurité des systèmes d'information.
…Décret n° 2015-349 du 27 mars 2015 relatif à l'habilitation et à l'assermentation des agents de l'autorité nationale de sécurité des systèmes d'information et pris pour l'application de l'article L. 2321-3 du code de la défense

[40] « Art. L. 246-2.-I. — Les informations ou documents mentionnés à l'article L. 246-1 sont sollicités par les agents individuellement désignés et dûment habilités des services relevant des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget, chargés des missions prévues à l'article L. 241-2.
http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&dateTexte=&categorieLien=id

Article L241-2
Peuvent être autorisées, à titre exceptionnel, dans les conditions prévues par l'article L. 242-1, les interceptions de correspondances émises par la voie des communications électroniques ayant pour objet de rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de l'article L. 212-1.
http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=3F9381B8793BF77416D293FEDEE176BC.tpdila10v_3?idArticle=LEGIARTI000028345000&cidTexte=LEGITEXT000025503132&categorieLien=id&dateTexte=20150418

à comparer au L 34-1-1 remplacé :

Article L34-1-1
Afin de prévenir les actes de terrorisme, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions peuvent exiger des opérateurs et personnes mentionnés au I de l'article L. 34-1 la communication des données conservées et traitées par ces derniers en application dudit article.
http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=3F9381B8793BF77416D293FEDEE176BC.tpdila10v_3?idArticle=LEGIARTI000028345117&cidTexte=LEGITEXT000006070987&categorieLien=id&dateTexte=20141231

[41] P. Cohet, Loi de Programmation Militaire 2014-2019 : Eléments d'évaluation du risque législatif lié à l'article 13. IFREI 2013.

[42] IV. — Tarifs hors taxes applicables à la fourniture de données par les opérateurs de communications électroniques.

CATÉGORIES DE DONNÉES	CODE	PRESTATIONS REQUISES	TARIFS
	WA 0X	A partir d'une demande dématérialisée conforme sur des adresses IP horodatées, rechercher sommairement dans le SI le plus pertinent les éléments d'identification relatifs à la personne physique, à l'installation, à la connexion, au contrat et aux identifications numériques.	De 1 à 20 : 4 € Au-dessus de 20 : 0,18 € par IP
	WA 0H	A partir d'une demande accompagnée d'un fichier électronique copiable, rechercher sommairement dans le SI le plus pertinent les éléments d'identification relatifs à la personne physique, à l'installation, à la connexion, au contrat et aux identifications numériques.	1 et 20 IP : 6,10 € Au-dessus de 20 : 0,28 € par IP
	WA 01	A partir d'une adresse IP horodatée et d'informations complémentaires, obtenir les éléments d'identification relatifs à la personne physique, à l'installation, à la connexion, au contrat et aux identifications numériques.	18 €
	WA 07	A partir de caractéristiques de compte, obtenir les éléments d'identification relatifs à la personne physique, à l'installation, à la connexion, au contrat et aux identifications numériques.	15,70 €
	WA 08	A partir d'une adresse courriel, obtenir les éléments d'identification relatifs à la personne physique, à l'installation, à la connexion, au contrat et aux identifications numériques.	15,70 €
	WA 09	A partir d'une adresse URL de site visité horodatée, obtenir les éléments d'identification relatifs à la personne physique, à l'installation, à la connexion, au contrat et aux identifications numériques.	15,70 €

	WI 01	Interception du trafic DATA/ IP émis et à destination de l'accès internet, à partir d'éléments caractéristique du compte (identité, adresse IP horodatée...) mettre en place l'interception du trafic DATA/ IP sur la période demandée spécifiant les caractéristiques de renvoi.	24 €

[43] Pascal Cohet. Black swans, red herrings : Analyse infocindynique d'un scénario de bifurcation des cyber-luttes. IFREI 2013.

[44] http://www.lebardegandi.net/post/2015/04/16/Loi-sur-le-renseignement-suite-mais-pas-fin

Loi sur le renseignement, vote de l'amendement de l'article L 851-4.

16 AVRIL 2015, PARIS, FRANCE

Le groupement d'hébergeurs qui avait signé le 10 avril dernier un communiqué conjoint appelant M. Manuel Valls à reconsidérer le projet de loi sur le renseignement débattu depuis lundi à l'Assemblée Nationale, a rencontré hier M. Bernard Cazeneuve, M. Emmanuel Macron et Mme Axelle Lemaire.

A l'issue de cette réunion, des engagements concrets quant à la préservation des données personnelles et au caractère ciblé, limité dans le temps et non systématique de ce dispositif de surveillance ont été apportés. Cette concertation tardive a permis d'aboutir à l'amendement de l'article L. 851-4 débattu et voté hier soir.

L'AFHADS, IDS, Ikoula, Gandi, Lomaco, Online & OVH, présents lors de cette réunion, resteront extrêmement vigilants dans les 18 mois à venir quant à l'application et l'utilisation de ce nouveau dispositif.

http://fr.gandi.press/99991-loi-sur-le-renseignement-vote-de-l-amendement-de-l-article-l-851-4

[45] http://www.lebardegandi.net/post/2015/04/17/Comment-la-loi-sur-le-renseignement-est-elle-cens%C3%A9e-s-appliquer-pour-les-h%C3%A9bergeurs

[46] Après la seconde occurrence de la référence :

« L. 851-1 »,

Rédiger ainsi la fin de l'alinéa 14 :

« . Dans le respect du principe de proportionnalité, l'autorisation du Premier ministre précise le champ technique de la mise en œuvre de ces traitements. Cette dernière ne permet pas de procéder à l'identification des personnes auxquelles ces informations ou documents se rapportent, ni au recueil d'autres données que celles qui répondent aux critères de conception des traitements automatisés. Les conditions prévues à l'article L. 861-3 sont applicables aux opérations matérielles effectuées pour cette mise en œuvre par les opérateurs et les personnes mentionnés à l'article L. 851-1. Les dispositions de l'article L. 821-5 ne sont pas applicables à cette technique de renseignement. »

EXPOSÉ SOMMAIRE

Le dispositif prévu à l'article L.851-4 du code de la sécurité intérieure a suscité des débats.

Dans ce contexte, le gouvernement a tenu des discussions avec les hébergeurs de sites Internet.

Le gouvernement est attaché à soutenir la compétitivité d'un secteur en croissance et qui crée des emplois dans notre pays et qui repose sur la confiance des clients et des utilisateurs. Rien dans le projet de loi n'entrave le développement de ces entreprises stratégiques.

Dans ce contexte, il est ressorti des discussions que le Gouvernement a eues avec les hébergeurs de sites internet que des précisions et des assurances supplémentaires pouvaient être de nature à clarifier les conditions de mise en œuvre de cette technique de renseignement.

A cet égard, le présent amendement prévoit que :

- L'autorisation du Premier ministre précisera le champ technique de la mise en œuvre de la mesure, qui sera, en vertu du principe de proportionnalité, limité aux éléments strictement nécessaires à la détection d'une menace terroriste
- Les opérateurs auront la possibilité, ainsi que le précise le renvoi à l'article L.861-3 du code de la sécurité intérieure, de s'assurer par eux-mêmes que les données de contenu seront exclues de la mise en œuvre de ces traitements.
- Enfin, le présent amendement énonce que la procédure d'urgence n'est pas applicable au dispositif.

http://www.assemblee-nationale.fr/14/amendements/2697/AN/437.asp

[47] http://www.01net.com/editorial/652616/loi-sur-le-renseignement-lhebergeur-altern-org-va-quitter-la-france/

[48] Pascal Cohet. Black swans, red herrings : Analyse infocindynique d'un scénario de bifurcation des cyber-luttes. IFREI 2013.

[49] Conférence de M. Jean-Jacques Urvoas à l'ENSP, 18 avril 2015, publié par le Ministère de l'intérieur le 19 avril sur Dailymotion : http://www.dailymotion.com/video/x2n42le

[50] Op. cit.

[51] Audition de l'auteur à Bercy, en présence de représentants du Syndicat de la magistrature et de Reporters sans frontières.

[52] http://www.zdnet.fr/actualites/lcen-le-conseil-constitutionnel-censure-l-amendement-devedjian-39157007.htm

[53] Cf. l'article de Girardeau : http://ecrans.liberation.fr/ecrans/2008/12/17/le-csa-et-internet-c-est-toute-une-histoire_957206

[54] http://lexpansion.lexpress.fr/high-tech/cyber-revolte-contre-le-csa_496502.html

[55] P. Cohet, Loi de Programmation Militaire 2014-2019 : Eléments d'évaluation du risque législatif lié à l'article 13. IFREI 2013.

[56] «

ARTICLE 1ER

A. Rédiger comme suit les I et II de cet article :

I.- L'article 1er de la loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication est ainsi rédigé :

« Art. 1er - La communication au public par voie électronique est libre.

« L'exercice de cette liberté ne peut être limité que dans la mesure requise, d'une part, par le respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et d'opinion et, d'autre part, par la sauvegarde de l'ordre public, par les besoins de la défense nationale, par les exigences de service public, par les contraintes techniques inhérentes aux moyens de communication, ainsi que par la nécessité, pour les services audiovisuels, de développer la production audiovisuelle.

« Les services audiovisuels comprennent les services de communication audiovisuelle telle que définie à l'article 2 de la présente loi ainsi que l'ensemble des services mettant à disposition du public ou d'une catégorie de public des œuvres audiovisuelles, cinématographiques ou sonores, quelles que soient les modalités techniques de cette mise à disposition. »

II.- L'article 2 de la loi n°86-1067 du 30 septembre 1986 précitée est ainsi rédigé :

« Art. 2 - On entend par communications électroniques les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique.

« On entend par communication au public par voie électronique toute mise à disposition du public ou de catégories de public, par un procédé de communication électronique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée.

« On entend par communication audiovisuelle toute communication au public de services de radio ou de télévision, quelles que soient les modalités de mise à disposition auprès du public, ainsi que toute communication au public par voie électronique de services autres que de radio et de télévision et ne relevant pas de la communication au public en ligne.

« Est considéré comme service de télévision tout service de communication au public par voie électronique destiné à être reçu simultanément par l'ensemble du public ou par une catégorie de public et dont le programme principal est composé d'une suite ordonnée d'émissions comportant des images et des sons.

« Est considéré comme service de radio tout service de communication au public par voie électronique destiné à être reçu simultanément par l'ensemble du public ou par une catégorie de public et dont le programme principal est composé d'une suite ordonnée d'émissions comportant des sons. »

B. Compléter in fine cet article par un IV ainsi rédigé :

IV - Ainsi qu'il est dit à l'article 1er de la loi n° 86-1067 du 30 septembre 1986 précitée, la communication au public par voie électronique est libre.

L'exercice de cette liberté ne peut être limité que dans la mesure requise, d'une part, par le respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et d'opinion et, d'autre part, par la sauvegarde de l'ordre public, par les besoins de la défense nationale, par les exigences de service public, par les contraintes techniques inhérentes aux moyens de communication, ainsi que par la nécessité, pour les services audiovisuels, de développer la production audiovisuelle.

On entend par communication au public par voie électronique toute mise à disposition du public ou de catégories de public, par un procédé de communication électronique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée.

On entend par communication au public en ligne toute transmission, sur demande individuelle, de données numériques n'ayant pas un caractère de correspondance privée, par un procédé de communication électronique permettant un échange réciproque d'informations entre l'émetteur et le récepteur.

On entend par courrier électronique tout message, sous forme de texte, de voix, de son ou d'image, envoyé par un réseau public de communication, stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère.

»
http://www.senat.fr/amendements/2003-2004/144/Amdt_2.html

[57] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:fr:HTML

[58] «
Article 14
Hébergement
1. Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le prestataire ne soit pas responsable des informations stockées à la demande d'un destinataire du service à condition que:
a) le prestataire n'ait pas effectivement connaissance de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages et intérêts, n'ait pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente
ou
b) le prestataire, dès le moment où il a de telles connaissances, agisse promptement pour retirer les informations ou rendre l'accès à celles-ci impossible.
2. Le paragraphe 1 ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle du prestataire.
3. Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation et n'affecte pas non plus la possibilité, pour les États membres, d'instaurer des procédures régissant le retrait de ces informations ou les actions pour en rendre l'accès impossible.
»
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:fr:HTML

[59] i.e. dépendant du type de service de communications électroniques envisagé : par exemple l'étude Hogan de 2011 pour l'ARCEP, relative à la détermination du périmètre des opérateurs de communications électroniques, considère que Skype, pour sa partie logiciel à logiciel, n'est pas un service de communications électroniques.
http://www.arcep.fr/uploads/tx_gspublication/etude-Hogan-Analysys-juin2011.pdf

[60] http://www.legifrance.gouv.fr/affichCode.do;jsessionid=9D25B0FB84EBCF7E657A355C1620EE63.tpdila19v_3?idSectionTA=LEGISCTA000006150658&cidTexte=LEGITEXT000006070987&dateTexte=20150428

[61] « *The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point. Frequently the messages have meaning; that is they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of communication are irrelevant to the engineering problem.* »
C.E. Shannon. *A Mathematical Theory of Communication*, Reprinted with corrections from The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948.
http://cm.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf

[62] Pascal Cohet. Black swans, red herrings : Analyse infocindynique d'un scénario de bifurcation des cyber-luttes. IFREI 2013.

[63] enseigné mais non publié.

[64] « *Une épigramme, si elle est bonne? Qui peut le décider? On ne sait même pas toujours ce qu'il a voulu dire, le sournois.* »
Goethe (Épigrammes vénitiennes)

[65] Cf. l'une des premières références officielles à la main rouge, dans le rapport de la commission d'enquête sur les activités du Service d'Action Civique :
« M. *Alain Vivien : Est-il vrai que parmi ceux qui ont combattu à El Biar il y avait Jim Al Cheick* [sic]?
M. Pierre Lemarchand : Oui. C'était un cas spécial. Il n'était ni gaulliste, ni un ancien résistant.[…] Il était un ancien militant de la main rouge en Tunisie. »
(Rapport n°955 remis au Président de l'Assemblée Nationale le 17 juin 1982.)
Rapport de la commission d'enquête sur les activités du Service d'Action Civique, Tome 2, ISBN 2-85209-004-X.

[66] Cf. Lucien Bitterlin : « *L'action terroriste ça peut être autre chose, ce seront, à partir de décembre 1961, les opérations de plasticage que l'on va commettre nous quand la sécurité militaire va nous donner un certain nombre de petits paquets de plastics avec des détonateurs et des mèches lentes pour poser devant les cafés, qui sont connus comme des fiefs OAS. Et là, nous allons mener une opération qui va semer la confusion, nous allons faire sauter un certain nombre de cafés, comme le Tonton Ville, comme l'Automatic, en plein secteur OAS* »

France Culture, 20 août 1987

http://www.franceculture.fr/player/reecouter?play=4669686

[67] http://www.rfi.fr/afrique/20130706-tunisie-francois-hollande-veille-froisser-personne-fahrat-hached/

[68] http://www.huffpostmaghreb.com/2013/12/02/archives-farhat-hached_n_4372279.html

[69] « L'expression 'informations ou documents' date de la loi de 91. En 2004, la totalité de l'internet devient accessible aux interceptions de sécurité par le remplacement du mot 'télécommunications' par les mots 'communications électroniques'. A supposer que l'expression ait eu une définition précise en 1991 pour le domaine de la téléphonie, le législateur n'a pas apporté une extension de définition permettant de savoir ce qu'elle signifie pour le domaine internet. De même pour l'expression 'services de communications électroniques' qui reste vague, ainsi que pour le mot 'connexion' (*des références précises au modèle OSI aideraient sans doute à lever des incertitudes*, en particulier dans le cadre d'une éventuelle généralisation du routage IP par inspection profonde des paquets proposant des accès de type CALEA). »

P. Cohet, Loi de Programmation Militaire 2014-2019 : Eléments d'évaluation du risque législatif lié à l'article 13. IFREI 2013.

[70] S'il ne fait pas de Deep Packet Inspection.

[71] « VI.-Les données conservées et traitées dans les conditions définies aux III, IV et V portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux.

Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications. »

http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=E1A0571B63B33DFF167664EB3E8285D8.tpdila11v_1?idArticle=LEGIARTI000028345210&cidTexte=LEGITEXT000006070987&categorieLien=id&dateTexte=20150426

[72] http://www.lemonde.fr/politique/article/2015/04/20/renseignement-le-champ-de-la-loi-est-beaucoup-trop-etendu-pour-henri-guaino_4618924_823448.html