IFREI

Document de travail

Contenu :

1 Note d'évaluation de risque : Loi de Programmation Militaire 2014-2019 : Eléments d'évaluation du risque législatif lié à l'article 13.
Version du 6 décembre 2013

2 Annexes :

Lien architecture du droit de la communication ↔ interceptions de sécurité
8 décembre 2013

Risques sémantiques et amendement Hérisson à l'article 13
8 décembre 2013

Clarification des périmètres de surveillance et interceptions
10 décembre 2013

Vulnérabilité liée aux ambigüités dans l'éventualité d'une saisine
17 décembre 2013

Diffusion :

Auteur :

Pascal Cohet (IFREI)

Contact :

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

Remarque liminaire

Ce document de travail n'est pas initialement destiné à un large public, faisant appel à des concepts cindyniques décrits par une modélisation stricte, et supposés connus et maitrisés. Toutefois, un bref glossaire simplifié est proposé ci-dessous à destination des lecteurs non cindyniciens :

Acteur : organisation étudiée suivant cinq aspects : statistique (ses informations), épistémique (ses connaissances), téléologique (ses objectifs), nomique (les règles qu'elle doit suivre, quel qu'en soit le type), et axiologique (ses valeurs).

Dégénérescence : absence d'ordre ou de priorité sur un aspect (terme *non péjoratif*, issu du vocabulaire de la mécanique quantique).

Situation : ensemble d'acteurs concernés par un danger donné.

Spectre de situations : ensemble de situations relatives à des acteurs observateurs, chaque observateur ayant une perception propre de la situation (perspective), et une estimation propre de ce qu'elle devrait être dans l'idéal (prospective).

Déficits : écarts entre la situation perçue par un acteur, et ce qu'il estime qu'elle devrait être. Les lacunes sont un type particulier de déficits (exemples : lacunes épistémiques : zones non cartographiées et maîtrisées dans les connaissances ; lacunes nomiques : zones sans principes, règles ou fondamentaux permettant de réguler les rapports entre acteurs ; lacunes statistiques : absence de données sur les évènements significatifs passé).

Dissonances : écarts entre aspects de chaque acteur (les dissonances axiologiques étant les différences de valeurs des différents acteurs d'une situation).

Divergences : écarts entre prospectives de différents observateurs (les divergences topologiques étant les écarts entre composition en acteurs souhaitées de la situation, et les divergences nomiques représentant les choix différents de principes, règles ou fondamentaux permettant de réguler les rapports entre acteurs).

Disparités : écart entre perspectives de différents observateurs.

Déficits cindynamiques : pathologies des flux (opérationnels) immatériels (informations, connaissances,…) entre acteurs (par exemple : absence de flux d'acquisition d'informations i.e. de veille menant à une incapacité à modéliser les précurseurs des risques et donc à les détecter, ou absence de flux didactiques préparatoires i.e. absence de préparation pédagogique).

Puissance : capacité d'un acteur d'un spectre de situations (i.e. d'un champ de propensions) à imposer sa prospective (redistribution topologique de puissances : répartition nouvelle des puissances des différents acteurs du spectre considéré).

Horogénèse informationnelle : dynamique de la création de frontières entre informations ouvertes (publiques) et fermées (confidentielles).

Les lecteurs désireux d'approfondir pourront utilement consulter ces articles :

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.

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

Pascal COHET †

« Introduire par le biais d'un amendement dans un texte sur la programmation militaire une réforme de cette importance et ayant un caractère sensible dans l'opinion publique peut, en effet, présenter des inconvénients sur les plans politique et juridique. Une telle réforme serait susceptible – je ne le souhaite pas ! – de retarder l'adoption du projet de loi de programmation militaire, qui doit impérativement intervenir avant la fin de l'année. »

Jean-Louis Carrère, Sénat, 21 octobre 2013.

Nature du problème envisagé

Lors de l'examen du projet de loi de programmation militaire au Sénat le 21 octobre 2013, Jean-Louis Carrère évoquait un risque de retard à l'adoption du texte en raison de l'évolution de l'article 13[1], prévoyant initialement une simple clarification de l'encadrement de l'usage par les services de l'état de la géolocalisation en temps réel. Quelques éléments d'analyse permettent une première évaluation du risque conjecturé, en tenant compte des aspects chronologiques et de la puissance effective des acteurs impliqués.

Situation et propensions globales

Les problématiques soulevées par l'article 13 du projet de loi de programmation militaire (LPM) s'inscrivent dans un contexte marqué par plusieurs grandes tendances. Primo, le développement du réseau IP mondial et sa pervasivité : les connexions au réseau IP interviennent désormais à toute heure et en tout lieu, rythmant les comportements quotidiens de la population mondiale. Quantitativement, le volume d'informations échangées connaît un accroissement global quasi-exponentiel. Secundo, ce développement pervasif s'inscrit dans un contexte de globalisation, marqué par de nouvelles menaces, en particulier non étatiques. La prévention des actes terroristes est devenue une priorité globale : le cyberespace apparaît dans ce cadre à la fois comme une menace, et comme une opportunité. D'une part, les entités (potentiellement) terroristes trouvent dans le réseau IP un outil opérationnel, mais d'autre part les services y trouvent eux un outil de surveillance et prévention techniquement performant.

D'un point de vue cindynique, l'innovation crée continuellement des lacunes épistémiques (connaissances) et nomiques (règles, lois…), générant ainsi de nouvelles vulnérabilités : le développement du réseau IP, des technologies liées, et des services qui l'utilisent n'échappent pas à cette règle. Ainsi, le législateur est amené à encadrer les usages émergents, devant faire face à plusieurs difficultés : ne pas légiférer en retard par rapport à l'émergence des menaces (dans les faits : il est le plus souvent emmené dans la course poursuite de la dialectique réglementaire), et gérer une complexité croissante, en particulier dûe à des phénomènes de convergence comme celui de la convergence de la téléphonie et des TIC. D'un point de vue législatif, c'est exactement la difficulté rencontrée actuellement, avec la loi de 91 encadrant les interceptions de sécurité (ou 'administratives', ou 'extrajudiciaires') à la suite d'affaires liées à des écoutes téléphoniques d'une part, et d'autre part, depuis le début des années 2000, une succession de lois liées aux TIC et encadrant les accès judiciaires ou extrajudiciaires aux 'données' des utilisateurs du réseau IP.

Enfin, au plan des relations internationales, l'article 13 est plus ou moins directement lié à l'affaire Snowden, aux outils mis en place par la NSA, aux relations de cette dernière avec ses partenaires (en particulier européens), et – dans ce cadre – à de conjecturables pressions diplomatiques tendant à la protection du soft power des États-Unis, pouvant, si ce n'est dicter, du moins impacter la posture de l'exécutif.

Situation spécifique

La détermination des acteurs directement impliqués dans la situation spécifiquement liée à l'article 13 nécessite une mise en perspective historique de l'ensemble des textes connexes au bloc extrajudiciaire expérimental devant être transféré (/modifié et pérennisé) dans le code de la sécurité intérieure (cf. infra : diagramme de structuration législative). Deux grandes lignées législatives sont impliquées : l'une liée à la loi de 91 sur les interceptions de sécurité, destinée à encadrer les écoutes téléphoniques préalablement non encadrées (voire niées), et l'autre liée au développement du réseau IP et de

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

la société de l'information. Etant donné la convergence entre le monde de la téléphonie et celui de l'internet, il est même étonnant que ces deux lignées législatives ne se soient pas rencontrées plus tôt.

La loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications a été codifiée à droit constant, donnant naissance au code de la sécurité intérieure (CSI), par l'ordonnance n° 2012-351 du 12 mars 2012 relative à la partie législative du code de la sécurité intérieure. Si les débats sur les écoutes téléphoniques duraient depuis les années 70, notamment alimentés par les questions de Michel Rocard[2] à propos des activités du GIC, la réglementation n'intervint qu'en 1991 – en particulier – à la suite de la condamnation de la France par la Cour européenne de droits de l'homme en 1990[3], mentionnant une violation de l'article 8 de la Convention européenne des droits de l'homme[4].

Concernant internet, plusieurs lois ont mené depuis le début des années 2000 à deux grands dispositifs de surveillance :

- d'une part la conservation des données permettant l'**identification des contributeurs** (i.e. des personnes ayant contribué à la publication d'un contenu en ligne) par les FAI et les hébergeurs,
- et d'autre part les '**logs de connexion**', enregistrant pour une durée de un an les données techniques relatives aux connexions des internautes (mesure concernant la totalité de la population).

L'identification des contributeurs était prévue par l'article 43-9 de la loi n° 2000-719 du 1er août 2000 modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, mais les décrets d'application prévus n'ont jamais été publiés. Cette mesure a été reprise par l'article 6 (par la suite maintes fois modifié) de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) devant transposer la directive commerce électronique, la transposition ayant été marquée par d'intenses affrontements entre cyber-ONG et industries phonographiques, et une forte implication des fournisseurs d'accès ou hébergeurs. Le décret d'application prévu a été publié tardivement (i.e. sept ans plus tard : 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).

Les logs de connexion sont une conséquence des attentats du 11 septembre 2001, et ont été justifiés initialement comme une mesure urgente exceptionnelle et temporaire 'impérieusement nécessaire' à la lutte contre les activités terroristes lors de l'adoption de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne (LSQ). L'article 22[5] du texte limitait la durée du dispositif dans le temps, celui-ci devant expirer au 31 décembre 2003. L'article 31 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure (LSI) a pérennisé ce dispositif en supprimant la limitation dans le temps imposée par l'article 22 initial. Là encore, les décrets d'application ne voient le jour que des années plus tard, en 2006, avec la publication du décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques, ce qui mine la crédibilité du discours initial ayant servi à justifier le dispositif.

Si ces dispositifs de surveillance restaient 'judiciarisés', les choses vont changer à la suite des attentats de Madrid du 11 mars 2004 et de Londres du 7 juillet 2005, poussant à l'adoption de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers (LCT). L'article 6 de la LCT instaure en effet un accès **extrajudiciaire** :

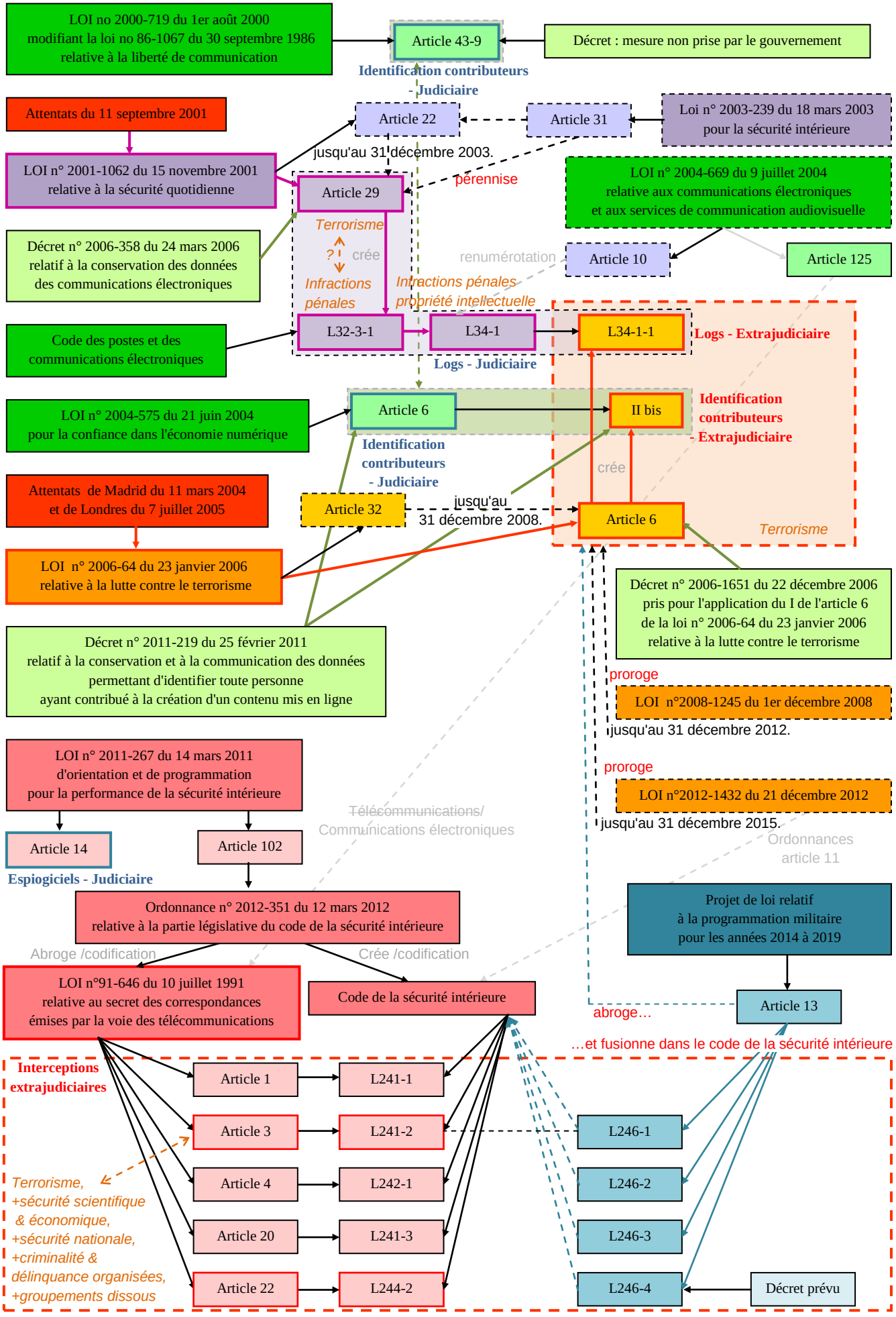
- aux données d'identification des contributeurs, par l'insertion d'un II bis à l'article 6 de la LCEN,
- et aux logs de connexion, par l'insertion d'un L 34-1-1 au L 34-1 du Code des postes et des communications électroniques (CPCE), lui-même découlant de l'article 29 de la LSQ.

Cet article constitue le bloc extrajudiciaire expérimental qui est au cœur de la problématique de l'article 13 de la LPM.

Tout comme pour la LSQ, ce dispositif anti-terroriste de la LCT est initialement temporaire (décrit comme 'expérimental' par la CNCIS[6]) et limité jusqu'au 31 décembre 2008 par son article 32. Il est prorogé une première fois jusqu'au 31 décembre 2012 par la loi n°2008-1245 du 1er décembre 2008, puis prorogé une seconde fois jusqu'au 31 décembre 2015 par la loi n°2012-1432 du 21 décembre 2012 (même si l'avis n° 56 (2013-2014) de M. Jean-Pierre Sueur, fait au nom de la commission des lois, mentionne une limite au 31 décembre 2014[7]). Alors que l'article 13 prévoyait initialement la prise en compte de la géolocalisation, le problème est qu'il vise maintenant à sortir le bloc extrajudiciaire expérimental (i.e. les mesures de l'article 6 de la LCT) de la LCEN et du CPCE pour le pérenniser (/modifier) dans le Code de la sécurité intérieure.

Eu égard à l'historique des textes précités, au-delà des services de l'Etat, les acteurs concernés par l'article 13 sont donc essentiellement les opérateurs et fournisseurs d'accès ou de services, et les cyber-ONG de plaidoyer, traditionnellement mobilisées sur ces thématiques.

Diagramme de structuration législative :



Divergences et conflictualité

S'agissant des acteurs privés, la seule réaction significative est celle de l'ASIC, groupe d'influence agissant en France, et regroupant des corporations internet dont Google et Facebook. L'ASIC a tenté de sensibiliser via une pétition online fustigeant l'article 13, dont il aurait dû être évident *a priori* qu'elle ne pourrait qu'être un échec. De fait, au 5 décembre seulement 29 personnes ont signé cette pétition, Google ou Facebook n'étant sans doute pas les entités les mieux placées aux yeux des internautes pour prétendre s'ériger en (adopter une posture de) défenseurs des données personnelles. L'avis semble être partagé par Fleur Pellerin, répondant à cette question du Monde le 4 décembre :

« *Les géants américains de l'Internet disent pourtant être victimes des Etats qui veulent surveiller la sphère numérique ?*

Ils tentent de se parer de vertu. C'est ce qu'ils ont essayé de faire en voulant forcer l'administration américaine à publier toutes les requêtes [de renseignement] et en nous enjoignant, en France, via l'Association des services Internet communautaires (ASIC), de faire un moratoire sur le projet de loi de programmation militaire [qui donne de nouveaux pouvoirs d'accès aux données d'internautes] alors qu'ils sont les premiers collecteurs mondiaux de données personnelles. On voit bien qu'ils sont dans une sorte de jeu de rôle où ils essayent de se mettre du côté des défenseurs des libertés et de tourner les principes à leur avantage. Il y a quelques années, ils faisaient la même chose avec la neutralité du Net, ce qui était déjà pour eux un moyen d'échapper à la régulation. »

Pour autant, un point particulier est intéressant dans la note relative au Projet de Loi de programmation militaire 2014 - 2019 du 3 décembre 2013 publiée par l'ASIC :
« *La nouvelle formulation retenue par le Projet de Loi de programmation militaire étend très largement le cadre actuel puisqu'elle vise non seulement les données techniques ("y compris les données techniques") mais aussi plus largement toute "information ou document" stockés par l'hébergeur. Ce mécanisme revient à offrir aux autorités, sans aucun contrôle préalable, un accès à tout document et/ou contenu stocké par un hébergeur sur ces serveurs. En outre, cet accès est prévu en "temps réel", par "sollicitation du réseau", ce qui revient à avoir un accès direct et permanent aux serveurs de l'hébergeur.*[…] *Ainsi, et sans les garanties offertes par le régime juridique des perquisitions, il sera dorénavant possible à ces autorités et pour les finalités visées, d'avoir accès – par exemple - à tous les documents stockés dans un service de "cloud" souscrit par un internaute déterminé.* »

Cette remarque fait directement référence à la rédaction de l'article 13, introduisant le futur L 246-1 du CSI, et à l'expression "informations ou documents", expression qui, selon l'ASIC, pourrait faire référence à des documents stockés dans le 'cloud', le sous-entendu étant que cela menacerait le business-model de l'informatique nébuleuse. Or, l'expression en question date de la loi de 1991 – époque des listes rouges, et des autocommutateurs et minitels – et plus précisément de son article 22, devenu depuis le L 244-2 du CSI.

Si les décrets de la lignée des textes internet précités permettent d'avoir *a posteriori* une idée relativement précise des données judiciairement ou extrajudiciairement accessibles, il n'en va pas de même pour les "informations ou documents" mentionnés à l'article 22 de la loi de 91 : aucun texte public ne semble en mesure de préciser le sens et la portée *actuelle* de cette expression, à supposer que la question ait réellement été étudiée au fur et à mesure des évolutions des technologies et des usages.

Ainsi, la formulation du L 246-1 ne semble pas intelligible, *y compris* pour des spécialistes : c'est bien ce qui permet à l'ASIC d'interpréter le texte proposé. C'est surtout aussi une vulnérabilité pour le texte, dans la mesure où l'intelligibilité de la loi est un objectif à valeur constitutionnelle : une éventuelle censure du L 246-1 proposé mènerait sans doute à la suppression de la totalité de l'article 13.

L'année prochaine le roman 1984 de Georges Orwell fêtera ses 65 ans.
Voice of Russia

La scène des cyber-ONG de plaidoyer françaises directement concernées est relativement clairsemée depuis quelques années, ayant subi une redistribution topologique de puissances pour diverses raisons : que ce soit par disparition naturelle de certaines d'entre elles, pour des raisons de divergences topologiques, ou pour des procédures judiciaires en cours; et, à vrai dire, il n'en reste qu'une de visible (la 'quadrature').

Les cyber-ONG sont caractérisées par une forte dissonance axiologique avec les autres acteurs, leurs valeurs fondamentales étant essentiellement la défense de la vie privée et de l'accès à l'information : c'est même leur raison d'être (jonction téléologique-axiologique), et leur cœur de réflexion est *in fine* l'horogénèse informationnelle.

De façon (apparemment) étonnante, aucune réaction n'a été manifestée, à part un communiqué plus que tardif publié le 3 décembre, et n'ayant reçu, comme prévu, aucune couverture médiatique significative.

Pourtant, la situation (ou plutôt le spectre de situations) aurait dû être conflictuelle et mener à des opérations de contre influence (mise en œuvre d'opérateurs de contre-transformation) en raison de fortes divergences prospectives, la prospective[8] de la cyber-ONG survivante étant marquée par de fortes divergences nomiques avec les porteurs du texte, étant [très probablement, ou devant être] caractérisée (*a posteriori*, i.e. après prise de conscience de la situation de crise) par les éléments prospectifs suivants :

Le bloc extrajudiciaire expérimental était considéré depuis sa création comme un problème en soi : le fait de le fusionner dans le CSI posant des divergences supplémentaires, dont *a minima* :

1. parce qu'il rend définitives des mesures d'exception temporaires justifiées par le terrorisme,

2. parce que le champ des motifs est étendu, au-delà du terrorisme, aux quatre autres motifs prévu par l'article 3 de la loi de 91 (L 241-2 du CSI) : la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, la prévention de la criminalité et de la délinquance organisées, et la prévention de la reconstitution ou du maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées,

3. parce que la loi de 91 est individualisante (interception *a posteriori*, i.e. après autorisation, des communications d'un individu), alors que l'article 13 prévoit l'accès à des données recueillies *a priori* pendant un an sur la totalité de la population française : même si une future demande d'interception concerne un seul individu, c'est bien l'ensemble de la population qui voit son comportement numérique/quotidien enregistré de façon préventive,

4. parce que le statut (hybride/émergent) des méta-données est très particulier : il ne s'agit pas vraiment de correspondances ou de contenus de correspondances, ni non plus de simples données de connexion. Il s'agit surtout de données socio-comportementales, dont l'invasivité de l'acquisition est directement proportionnelle à la pervasivité des usages du réseau IP, permettant de connaître de façon particulièrement précise et exhaustive le comportement quotidien des individus,

5. parce que la rédaction du texte, mentionnant une '*sollicitation du réseau*' et prévoyant pour la CNCIS un '*accès permanent au dispositif de recueil des informations ou documents*', peut laisser craindre le déploiement de dispositifs d'interceptions à divers endroits du réseau IP, voire la légalisation *a posteriori* d'éventuels dispositifs déjà déployés sournoisement lors de la législature précédente par exemple sur les points d'atterrissage bretons ou marseillais des câbles sous-marins du réseau IP qui permettraient des échanges avec la NSA.

Sauf exception, cette prospective est assez divergente de celle de la plupart des professionnels des médias ayant fait l'effort de se pencher un peu sur le problème, et pour lesquels l'article 13 n'introduirait rien de vraiment nouveau, marquant une disparité de perceptions révélatrice de difficultés à percevoir la situation 'en soi' (le point important étant la conséquence pratique de ces difficultés : un blocage des leviers de sensibilisation du public, et, partant, de canalisation des volontés politiques).

Par ailleurs, concernant l'article 14 que personne n'évoque publiquement, une analyse moins superficielle et plus approfondie des divers sous-acteurs du cyber-activisme mènerait à devoir considérer que l'acceptation de la légalisation d'un hypothétique accès direct aux systèmes d'information des individus à des fins de neutralisation d'attaques (dont ni le début, ni l'origine ne sont définis) à partir de leurs postes qui pourraient être utilisés à ces fins à leur insu est tout sauf acquise, et ce d'autant plus que les responsables des systèmes d'information de l'état ou des opérateurs d'importance vitale ne sont pas eux-mêmes en mesure de garantir leur propre étanchéité. A cet égard, s'agissant de réduction de divergences prospectives, si l'intention de la mesure est plus précise il conviendrait sans doute de l'exprimer plus clairement, à des fins de réduction de conflictualité.

Si un tel état de choses se produit, aucun stratège, si ingénieux soit-il, ne saurait redresser la situation.
Sun Zi

Ainsi, la prospective cyber-ONG diverge potentiellement fortement de celle des porteurs ou partisans du projet de loi de programmation militaire. Pourtant, force est de constater l'inexistence de réactions avant l'adoption en première lecture par l'assemblée, et même une réaction plus précoce, et donc potentiellement humiliante, d'un groupe d'influence

comportant des corporations tirant des bénéfices substantiels de données comportementales des internautes. Une question importante est donc de comprendre comment la cyber-ONG survivante a pu subir un tel revers historique.

Si ce n'est l'état de panique, du moins la situation de crise rencontrée, résulte d'une lacune statistique résultant elle-même d'une part de probables lacunes épistémiques, et d'autre part d'un déficit cindynamique primaire : l'absence d'acquisition de flux informationnels qui auraient permis la détection précoce de signaux faibles (si tant est qu'ils puissent être considérés comme tels), comme la volonté clairement exprimée par Manuel Valls dès le 16 octobre 2012, lors de l'examen de la loi du 21 décembre 2012, de fusionner[9] la loi de 91 et le bloc extrajudiciaire de la LCT : « *Monsieur Hyest, je vous confirme que le Gouvernement adhère totalement à votre objectif d'unification des dispositifs de la loi de 1991 et de celle de 2006.* [...] *L'unification de ces dispositifs est tout à fait nécessaire. Une telle évolution serait d'ailleurs de bonne administration et faciliterait l'exercice par la Commission nationale de contrôle des interceptions de sécurité de ses pleines prérogatives, ainsi que vous l'avez dit tout à l'heure. Nous devons y être attentifs. Je ferai d'ailleurs moi-même des propositions en ce sens dans le cadre non seulement de l'élaboration, en cours, du Livre blanc sur la défense et la sécurité nationale, initiative lancée par le Chef de l'État, mais aussi de la mission d'information constituée par l'Assemblée nationale en vue d'évaluer le cadre juridique applicable à l'exercice des missions de renseignement. Je ne vois aucun inconvénient à ce que cette unification intervienne le plus rapidement possible et j'œuvrerai dans ce but.* ».

Ce déficit cindynamique est lui-même le résultat d'un déficit stratégique (téléologique) *de facto* : qu'il résulte d'une absence accidentelle de planification stratégique, ou d'une intention plus ou moins exprimée de tel ou tel sous-acteur de l'acteur considéré, même si par ailleurs les marges de manœuvre restreintes dans les opérations de contre-influence en France face à des directives ont pu mener à considérer la nécessité de concentrer les ressources sur les instances européennes. Au total, le résultat est une défection quasi-totale face à un texte français d'ampleur historique, et qui sera – d'une façon ou d'une autre – un exemple à l'échelle internationale, en particulier dans le cadre du feuilleton de l'affaire Snowden.

Ce déficit téléologique de fait a par ailleurs des conséquences aggravantes s'agissant de la gestion de la crise rencontrée : l'impossibilité d'aligner au pied levé des ETP formés de façon adaptée aux opérations d'influence parlementaire qu'il aurait fallu mener en France sur ce sujet (déficits épistémiques), et l'incapacité à mobiliser largement : lacunes épistémiques du public – voire des journalistes – non compensées par des flux didactiques préparatoires soutenus indispensables dans la durée pour des questions techno-législatives complexes, réduisant toute tentative de mobilisation à de simples opérations de propagande ou de manipulation de masse.

Dans de telles conditions d'impéritie, compte-tenu de ces déficits et du calendrier parlementaire prévu, toute opération de contre-transformation n'a pratiquement aucune chance d'aboutir : la LPM sera très probablement adoptée dans les temps sans modification substantielle de l'article 13. La seule porte de sortie tactique reste une saisine du Conseil constitutionnel sur la base de l'inintelligibilité manifeste du L246-1, qui pourrait être contrée par des efforts de clarté rédactionnelle conjoints des acteurs de l'intérieur et de la défense. D'un point de vue plus général, la situation est marquée par d'importantes lacunes statistiques et épistémiques de très nombreux acteurs, contrastant fortement avec l'importance des enjeux, qui auraient mérité plus de dialogues, en particulier avec et au sein de la société civile.

P. Cohet.
6 décembre 2013

A noter : des annexes sont ajoutées progressivement, pour avoir la dernière version, télécharger depuis le site de l'IFREI :
Loi de Programmation Militaire 2014-2019 : Eléments d'évaluation du risque législatif lié à l'article 13

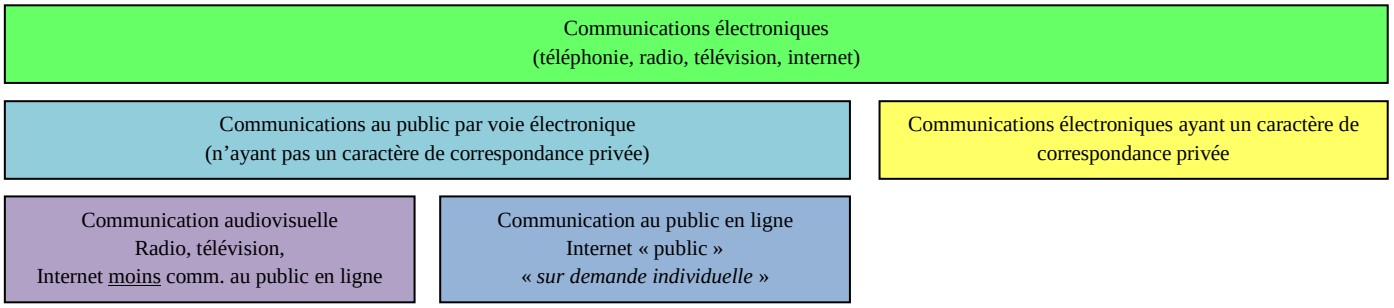
Annexe 1 : Lien architecture du droit de la communication ↔ interceptions de sécurité

En 2003, le projet de loi économie numérique (future LCEN), visant en particulier à transposer la directive 2000-31CE, prévoit initialement à son article 1 [10] de définir la communication sur internet comme un sous-ensemble de la communication audiovisuelle, et donc de la placer sous le pouvoir de régulation du CSA. Cette proposition rencontre de fortes oppositions, et finalement les sénateurs Hérisson et Sido proposent un amendement[11] – adopté en seconde lecture au Sénat – dessinant une nouvelle architecture constituée d'un linteau : la communication au public par voie électronique, s'appuyant sur deux piliers : la communication audiovisuelle et la communication au public en ligne.

L'amendement, adopté en séance le 8 avril 2004, et approuvé par Patrick Devedjian qui avait succédé à Nicole Fontaine, apporte une définition cruciale, celle de la communication électronique :

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

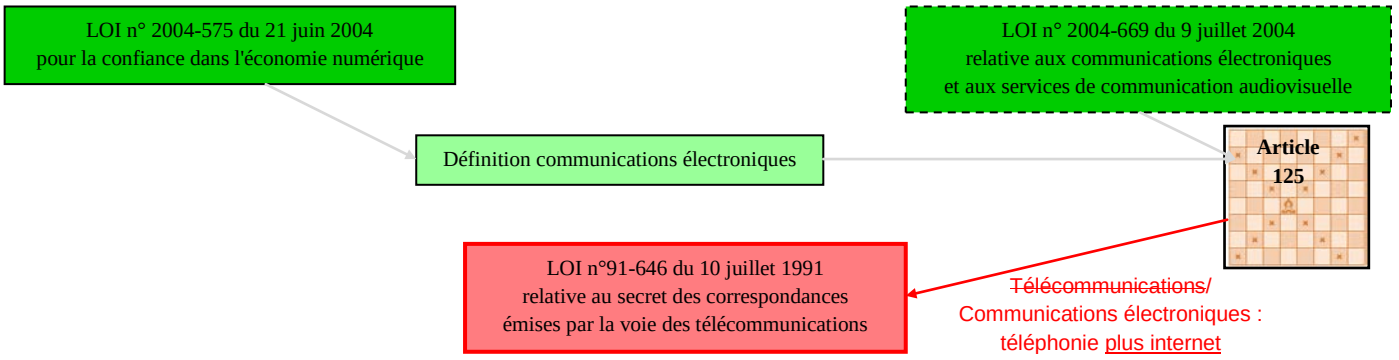
L'architecture globale se schématise alors ainsi :



La LCEN, promulguée en juin, est immédiatement suivie par la loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle (transposant le « paquet télécom [12]»). Son article 2 reprend la définition de l'amendement Hérisson :
« *Article 2* […] *Communications électroniques.*
«On entend par communications électroniques les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique.»; […] »

L'article 125 injecte cette définition dans la loi de 91 : « *Article 125*
La loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications est ainsi modifiée : 1° Dans le titre et dans les dispositions de la loi, le mot : «télécommunications» est remplacé par les mots : «communications électroniques»; […] »

Dès cet instant, la totalité de l'internet – correspondances privées comprises – est devenue accessible aux interceptions de sécurité. En matière de divergences prospective, s'agissant des cyber-ONG, en tous cas de celle ayant eu le lead stratégique sur l'opposition à la LCEN, cette mesure ne posait pas de problème, la position de principe étant le refus clair de toute surveillance *a priori* de l'ensemble de la population (logs de connexion) et l'acceptation, seulement, d'une surveillance ciblée *a posteriori* (i.e. pour des motifs légitimes et avérés) d'individus (interceptions ciblées).



Annexe 2 : Risques sémantiques et amendement Hérisson à l'article 13

Si vous ne vous rappelez plus où vous avez réveillonné l'année dernière, faites le 17.
G Moréas

La rédaction de l'article 13 (version transmise par l'assemblée pour la seconde lecture au Sénat) comporte quelques risques informationnels (sémantiques, et pouvant menacer *in fine* tant les services que le public), dont par exemple :

►« Art. L. 246-1. - Pour les finalités énumérées à l'article L. 241-2, peut être autorisé le recueil, auprès des opérateurs de *communications électroniques* et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, des *informations ou documents* traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de *connexion* à des *services* de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelant, la durée et la date des communications.[…] »

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[1]).

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

L'expression novatrice '*sollicitation du réseau*' intrigue certains acteurs qui imaginent qu'elle fait référence à (et permet de légaliser) un accès direct aux réseaux des opérateurs, c'est-à-dire à l'installation d'un dispositif physique permanent permettant la récupération des données circulant sur le réseau IP des opérateurs ou stockées sur les serveurs qui y sont reliés. De ce point de vue, l'amendement n° 2 du 6 décembre 2013[13] du sénateur Hérisson, qu'il soit adopté ou non, permettra probablement aux sénateurs d'apporter des précisions réduisant ce risque informationnel lors des débats publics : « *Alinéa 9*

Remplacer les mots : du réseau par les mots : de l'opérateur

Objet

Ce projet de disposition concerne le recueil d'informations par les personnes habilitées aux finalités énumérées à l'article L. 241-2. La méthode proposée pour permettre l'accès aux données sensibles, à savoir un raccordement direct aux réseaux des opérateurs, soulève de nombreuses difficultés de mise en œuvre car elle se distingue très nettement de celle habituellement utilisée et qui a pourtant fait ses preuves. […] »

Un risque informationnel majeur lié à un tel dispositif physique permanent s'il stockait *a priori* d'énormes quantités de données personnelles (notamment en ayant éventuellement accès à 12 mois glissants de logs de connexion de la population) est celui d'une véritable *marée noire informationnelle* en cas de fuite, soit une véritable catastrophe pour l'environnement informationnel.

[1] Communications Assistance for Law Enforcement Act

Annexe 3 : Clarification des périmètres de surveillance et interceptions

L'identification des contributeurs est prévue depuis la loi du 1er aout 2000, et confirmée par la LCEN en 2004. Elle impose aux FAI et hébergeurs de conserver les données permettant d'identifier toute personne ayant contribué à la publication d'un contenu sur internet. Le problème adressé est celui du droit de la communication (diffamation,…).

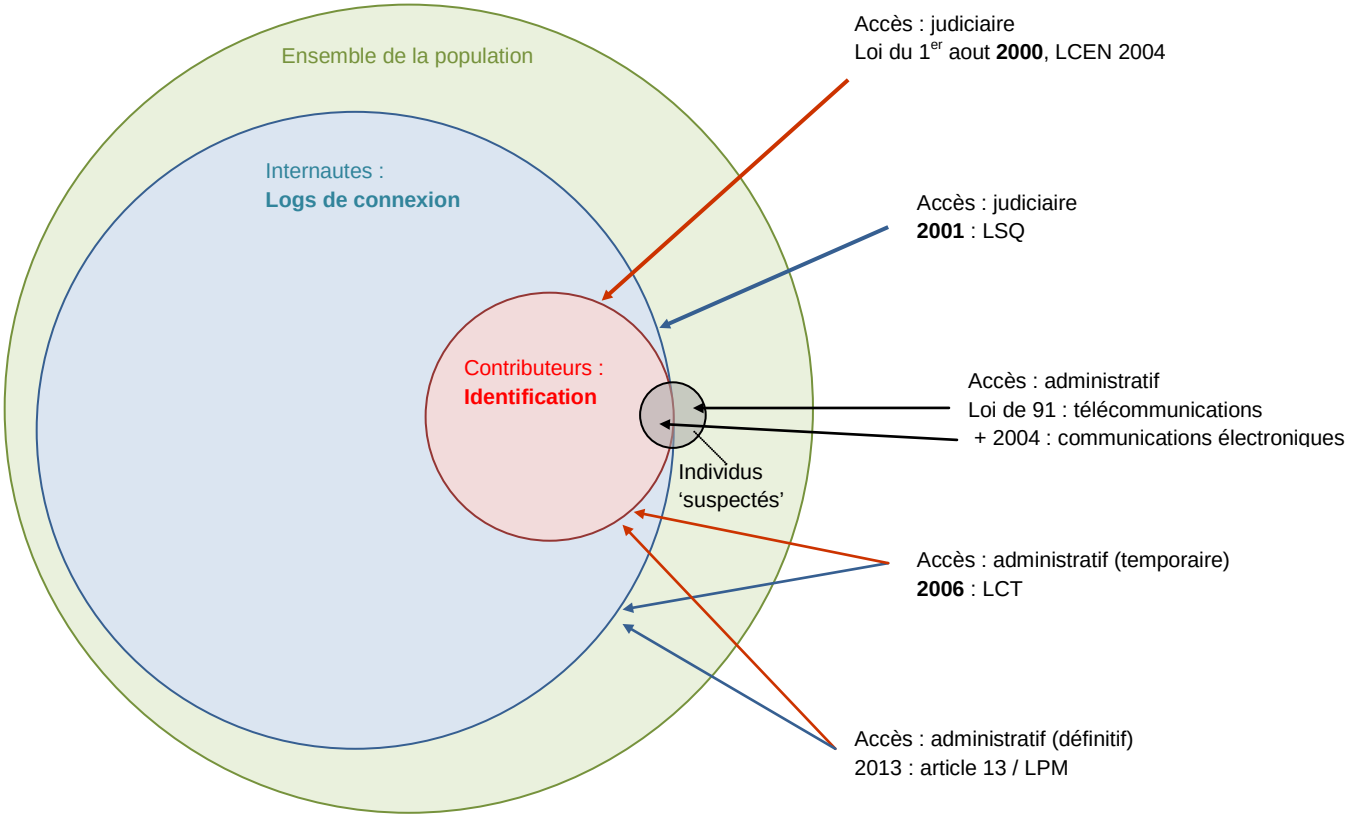
Les logs de connexion sont prévus depuis la LSQ, et imposent la conservation pour une durée de un an des données de connexion de l'ensemble de la population. Le problème adressé est celui des moyens de la lutte anti-terroriste.

Données d'identification des contributeurs et logs de connexion du public sont initialement accessibles par les juges.

L'incorporation du domaine internet à la loi de 91 intervient en 2004, cette loi conservant son esprit : interception ciblée, après autorisation administrative.

La LCT autorise un accès administratif aux logs de connexion et aux données d'identification en 2006, à titre temporaire.

L'article 13 de la LPM prévoit de pérenniser l'accès administratif aux logs de connexion et aux données d'identification des contributeurs en l'injectant dans la loi de 91 devenue CSI.

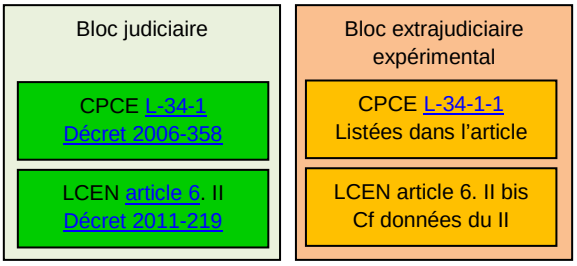


Annexe 4 : Vulnérabilité liée aux ambigüités dans l'éventualité d'une saisine

Great part of the information obtained in War is contradictory, a still greater part is false, and by far the greatest part is of a doubtful character
Clausewitz

La fusion du bloc extrajudiciaire expérimental de la LCT dans le CSI a soulevé des interrogations quant à la nature des données de connexion et d'identification évoquées par le L 246-1 créé par l'article 20 (ex 13) de la LPM, qui deviennent du fait de la rédaction (…'*y compris*'…) un sous-ensemble des '*informations ou documents*' prévus dès la loi de 91, et qui n'ont jamais désigné les contenus des correspondances interceptées.

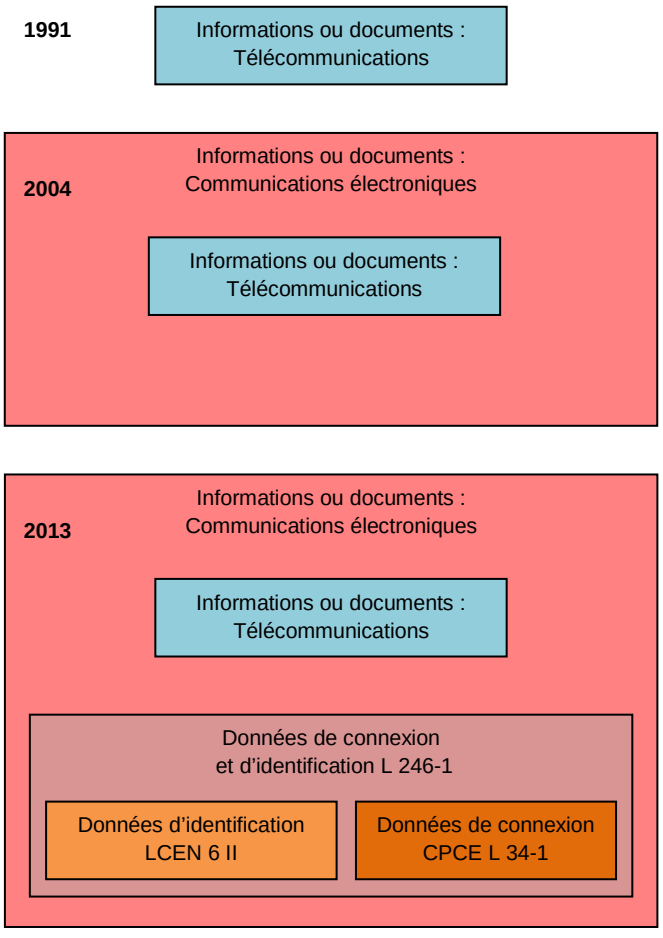
Le problème de la définition du périmètre de ces données comportementales est d'autant plus sensible que l'effet majeur – en termes de proportionnalité – de l'article 20 est de rendre définitive une mesure existante temporaire et exceptionnelle deux fois prorogée.



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[14] 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[15] : 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.

L'extension du périmètre global du dispositif d'interceptions loi de 91/CSI peut se schématiser alors ainsi :



La loi de 91 a pour objectif essentiel d'encadrer les interceptions extrajudiciaires ciblées de communications. Les services peuvent accéder aux '*informations ou documents*' nécessaires à ces interceptions de contenus ('*écoutes*').

En 2004, la loi de 91 (qui sera codifiée en 2012 dans le CSI) est étendue à l'ensemble des *communications électroniques*[16] (téléphonie + internet).

Aucun texte ne précise le sens de l'expression '*informations ou documents*' pour ce qui concerne internet. On peut encore estimer que le CSI concerne des interceptions *ciblées*.

En 2013 la LPM incorpore les données de connexion et d'indentification au CSI. L'accès extrajudiciaire à ces données qui existait à titre exceptionnel depuis 2006 est pérennisé.

Jean-Louis Carrère précise que ces données sont celles prévues au L 34-1 du CPCE et au II de l'article 6 de la LCEN.

Le dispositif repose sur l'enregistrement *a priori* des données de l'ensemble de la population, qui sont désormais un sous-ensemble des '*informations ou documents*', tout en étant une source première de renseignements, et non plus seulement nécessaires aux interceptions.

Une ambigüité demeure, le sens de l'expression '*informations ou documents*' n'étant toujours pas précisé depuis 2004.

[1] Texte adopté à l'assemblée en première lecture par l'Assemblée nationale le 3 décembre 2013 :
« **Article 13**
I. – Le livre II du code de la sécurité intérieure est ainsi modifié :
1° L'intitulé du titre IV est complété par les mots : « et accès administratif aux données de connexion » ;
2° Il est ajouté un chapitre VI ainsi rédigé :
« Chapitre VI
« Accès administratif aux données de connexion
« *Art. L. 246-1*. – Pour les finalités énumérées à l'article L. 241-2, peut être autorisé le recueil, auprès des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, des **informations ou documents** traités ou conservés par leurs réseaux ou services de communications électroniques, **y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelant, la durée et la date des communications**.
« *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.
« II. – Les demandes des agents sont motivées et soumises à la décision d'une personnalité qualifiée placée auprès du Premier ministre. Cette personnalité est désignée pour une durée de trois ans renouvelable par la Commission nationale de contrôle des interceptions de sécurité, sur proposition du Premier ministre qui lui présente une liste d'au moins trois noms. Des adjoints pouvant la suppléer sont désignés dans les mêmes conditions. La personnalité qualifiée établit un rapport d'activité annuel adressé à la Commission nationale de contrôle des interceptions de sécurité. Ces décisions, accompagnées de leur motif, font l'objet d'un enregistrement et sont communiquées à la Commission nationale de contrôle des interceptions de sécurité.
« *Art. L. 246-3*. – Pour les finalités énumérées à l'article L. 241-2, les informations ou documents mentionnés à l'article L. 246-1 peuvent être recueillis sur sollicitation du réseau et transmis en temps réel par les opérateurs aux agents mentionnés au I de l'article L. 246-2.
« L'autorisation de recueil de ces informations ou documents est accordée, sur demande écrite et motivée des ministres de la sécurité intérieure, de la défense, de l'économie et du budget ou des personnes que chacun d'eux a spécialement désignées, par décision écrite du Premier ministre ou des personnes spécialement désignées par lui, pour une durée maximale de trente jours. Elle peut être renouvelée, dans les mêmes conditions de forme et de durée. Elle est communiquée dans un délai de quarante-huit heures au président de la Commission nationale de contrôle des interceptions de sécurité.
« Si celui-ci estime que la légalité de cette autorisation au regard des dispositions du présent titre n'est pas certaine, il réunit la commission, qui statue dans les sept jours suivant la réception par son président de la communication mentionnée au deuxième alinéa.
« Au cas où la commission estime que le recueil d'une donnée de connexion a été autorisé en méconnaissance des dispositions du présent titre, elle adresse au Premier ministre une recommandation tendant à ce qu'il y soit mis fin.
« Elle porte également cette recommandation à la connaissance du ministre ayant proposé le recueil de ces données et du ministre chargé des communications électroniques.
« *Art. L. 246-4*. – La Commission nationale de contrôle des interceptions de sécurité dispose d'un accès permanent au dispositif de recueil des informations ou documents mis en œuvre en vertu du présent chapitre, afin de procéder à des contrôles visant à s'assurer du respect des conditions fixées aux articles L. 246-1 à L. 246-3. En cas de manquement, elle adresse une recommandation au Premier ministre. Celui-ci fait connaître à la commission, dans un délai de quinze jours, les mesures prises pour remédier au manquement constaté.
« Les modalités d'application du présent article sont fixées par décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés et de la Commission nationale de contrôle des interceptions de sécurité, qui précise notamment la procédure de suivi des demandes et les conditions et durée de conservation des informations ou documents transmis.
« *Art. L. 246-5*. – Les surcoûts identifiables et spécifiques éventuellement exposés par les opérateurs et personnes mentionnées à l'article L. 246-1 pour répondre à ces demandes font l'objet d'une compensation financière de la part de l'État. » ;
3° Les articles L. 222-2, L. 222-3 et L. 243-12 sont abrogés ;
4° À la première phrase du premier alinéa de l'article L. 243-7, les mots : « de l'article L. 243-8 et au ministre de l'intérieur en application de l'article L. 34-1-1 du code des postes et des communications électroniques et de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique » sont remplacés par les références : « des articles L. 243-8, L. 246-3 et L. 246-4 » ;
5° À l'article L. 245-3, après le mot : « violation », sont insérées les références : « des articles L. 246-1 à L. 246-3 et ».
II, III et IV. – *(Non modifiés)* »

Pour le II, III et IV, cf : Article adopté en première lecture par le Sénat le le 21 octobre 2013:

« **Article 13**

I. - Le titre IV du livre II du code de la sécurité intérieure est ainsi modifié :

1° L'intitulé est ainsi rédigé : « Interceptions de sécurité et accès administratif aux données de connexion » ;

2° Est ajouté un chapitre VI ainsi rédigé :

« CHAPITRE VI

« Accès administratif aux données de connexion

« *Art. L. 246-1*. - Pour les finalités énumérées à l'article L. 241-2, peut être autorisé le recueil, auprès des opérateurs de communications électroniques et personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des prestataires mentionnés 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 communication électronique, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communication électronique, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelant, la durée et la date des communications.

« *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.

« II. - Les demandes des agents sont motivées et soumises à la décision d'une personnalité qualifiée placée auprès du Premier ministre. Cette personnalité est désignée pour une durée de trois ans renouvelable par la Commission nationale de contrôle des interceptions de sécurité sur proposition du Premier ministre qui lui présente une liste d'au moins trois noms. Des adjoints pouvant la suppléer sont désignés dans les mêmes conditions. La personnalité qualifiée établit un rapport d'activité annuel adressé à la Commission nationale de contrôle des interceptions de sécurité. Les décisions, accompagnées de leur motif, font l'objet d'un enregistrement et sont communiquées à la Commission nationale de contrôle des interceptions de sécurité.

« *Art. L. 246-3*. - Pour les finalités énumérées à l'article L. 241-2, les données prévues à l'article L. 246-1 peuvent être recueillies sur sollicitation du réseau et transmises en temps réel par les opérateurs aux agents mentionnés au I de l'article L. 246-2.

« L'autorisation est accordée, sur demande écrite et motivée des ministres de la sécurité intérieure, de la défense, de l'économie et du budget ou des personnes que chacun d'eux aura spécialement désignées, par décision écrite du Premier ministre ou des personnes spécialement désignées par lui, pour une durée maximale de dix jours. Elle peut être renouvelée dans les mêmes conditions de forme et de durée. Elle est communiquée dans un délai de quarante-huit heures au président de la Commission nationale de contrôle des interceptions de sécurité.

« Si celui-ci estime que la légalité de cette décision au regard des dispositions du présent titre n'est pas certaine, il réunit la commission, qui statue dans les sept jours suivant la réception par son président de la communication mentionnée au premier alinéa.

« Au cas où la commission estime que le recueil d'une donnée de connexion a été autorisé en méconnaissance des dispositions du présent titre, elle adresse au Premier ministre une recommandation tendant à ce qu'il y soit mis fin.

« Elle porte également cette recommandation à la connaissance du ministre ayant proposé le recueil de ces données et du ministre chargé des communications électroniques.

« *Art. L. 246-4*. - La Commission nationale de contrôle des interceptions de sécurité dispose d'un accès permanent au dispositif de recueil de données techniques mis en oeuvre en vertu du présent chapitre afin de procéder à des contrôles visant à s'assurer du respect des conditions fixées aux articles L. 246-1 à L. 246-3. En cas de manquement, elle adresse une recommandation au Premier ministre. Celui-ci fait connaître à la commission, dans un délai de quinze jours, les mesures prises pour remédier au manquement constaté.

« Les modalités d'application du présent article sont fixées par décret en Conseil d'État après avis de la Commission nationale de l'informatique et des libertés et de la Commission nationale des interceptions de sécurité, qui précise notamment la procédure de suivi des demandes et les conditions et durée de conservation des données transmises.

« *Art. L. 246-5*. - Les surcoûts identifiables et spécifiques éventuellement exposés par les opérateurs et personnes mentionnées au premier alinéa pour répondre à ces demandes font l'objet d'une compensation financière. » ;

3° Les articles L. 222-2, L. 222-3 et L. 243-12 sont abrogés ;

4° À la première phrase du premier alinéa de l'article L. 243-7, les mots : « de l'article L. 243-8 et au ministre de l'intérieur en application de l'article L. 34-1-1 du code des postes et des communications électroniques et de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique » sont remplacés par les références : « des articles L. 243-8, L. 246-3 et L. 246-4 » ;

5° À l'article L. 245-3, après les mots : « en violation », sont insérés les mots : « des articles L. 246-1 à L. 246-3 et ».

II. - L'article L. 34-1-1 du code des postes et des communications électroniques est abrogé.

III. - Le II *bis* de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique est abrogé.

IV. - Le présent article entre en vigueur le 1er janvier 2015.»

[2]« M. Rocard demande à M. le ministre d'Etat chargé de la défense nationale :
1° s'il est exact que, dans une caserne des pompiers dépendant du gouvernement militaire de Paris et située 2bis, rue de Tourville, fonctionne le centre d'écoute téléphonique de la région parisienne, baptisé « Groupement interministériel de contrôle » ;
2° s'il est exact que cet organisme est placé sous l'autorité d'un officier supérieur du S.D.E.C.E., c'est-à-dire sous le contrôle permanent du ministre d'Etat chargé de la Défense nationale;
3° s'il est exact que des enregistrements téléphoniques soient écoutés et reproduits par diverses personnes ne dépendant pas du ministre de la Défense nationale, ni même parfois du ministre de l'Intérieur;
4° quelles sont les personnes qui ont droit à l'utilisation de ces écoutes téléphoniques;
5° s'il ne craint pas qu'en la circonstance, ces écoutes faites sans l'autorisation d'un juge d'instruction constituent une infraction grave aux prescriptions du code des P.T.T. et, en particulier, à son article 177. (Question du 8 juin 1971).

Réponse. — Au 2bis, avenue de Tourville, le seul service relevant du département de la Défense nationale est celui de la sécurité militaire dont les attributions, fixées par les règlements, excluent toute écoute téléphonique et d'une manière générale toute mesure non prévue par les lois en vigueur. »

[3] Roger Errera, *Les origines de la loi française du 10 juillet 1991 sur les écoutes téléphoniques*. http://www.rtdh.eu/pdf/2003851.pdf.

[4] « 1. toute personne a droit au respect de sa vie privée et familiale, de son domicile et se sa correspondance
2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

[5] Article 22

Afin de disposer des moyens impérieusement nécessaires à la lutte contre le terrorisme alimenté notamment par le trafic de stupéfiants et les trafics d'armes et qui peut s'appuyer sur l'utilisation des nouvelles technologies de l'information et de la communication, les dispositions du présent chapitre sont adoptées pour une durée allant jusqu'au 31 décembre 2003.

Le Parlement sera saisi par le Gouvernement, avant cette date, d'un rapport d'évaluation sur l'application de l'ensemble de ces mesures.

[6] La CNCIS distingue les deux régimes :
Le régime de l'article L. 244-2 du Code de la sécurité intérieure (ex-article 22 de la loi du 10 juillet 1991)
et :
Le dispositif expérimental de l'article 6 de la loi du 23 janvier 2006 (article L. 34-1-1 du Code des postes et des communications électroniques)
Commission nationale de contrôle des interceptions de sécurité, *20e rapport d'activité 2011-2012*. Février 2013.
http://www.ladocumentationfrancaise.fr/docfra/rapport_telechargement/var/storage/rapports-publics/134000156/0000.pdf

[7] « Notons que la Cour européenne des droits de l'homme, dans un arrêt du 2 septembre 20101, a estimé qu'un dispositif de géolocalisation pouvait être acceptable au regard du droit au respect de la vie privée garanti par l'article 8 § 1 de la convention européenne de sauvegarde des droits de l'homme, à condition que la loi soit très précise dans sa description du dispositif.
Se pose par ailleurs une difficulté au regard de l'insertion de ce dispositif au sein de notre législation.

En effet, le dispositif de droit commun s'agissant des interceptions de sécurité administratives (c'est-à-dire extrajudiciaires) n'est pas celui de l'article L. 34-1 du code des postes et télécommunications, inséré par la loi du 23 janvier 2006 et visé par le présent article, mais celui des articles L. 241-1 et suivants du code de la sécurité intérieure, issu de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, qui définit notamment les missions de la CNCIS. Le dispositif issu de la loi de 2006 constitue un système plus souple, mais moins protecteur des libertés, permettant de recueillir uniquement des données de connexion et seulement dans le cadre de la lutte anti-terroriste.

Or, d'une part **ce dispositif a été conçu comme temporaire et il doit devenir caduc le 31 décembre 2014**, après avoir été prorogé pour la troisième fois par la loi du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme précitée. À l'occasion de l'examen de ce texte à l'Assemblée nationale, le ministre de l'Intérieur s'était d'ailleurs engagé à proposer une fusion des deux dispositifs avant cette date. »

[8] Au sens infocindynique strict : Situation estimée idéale par la cyber-ONG analysée.

[9] « *Monsieur Hyest, je vous confirme que le Gouvernement adhère totalement à votre objectif d'unification des dispositifs de la loi de 1991 et de celle de 2006.*

Vous avez eu raison, d'ailleurs, de souligner qu'il ne s'agissait pas de lois d'exception. Ce point est très important car, si nous pouvons exprimer des différences les uns et les autres, dans la majorité ou dans l'opposition, ici ou à l'Assemblée nationale, la jurisprudence du juge constitutionnel est constante pour accompagner l'adaptation de notre arsenal législatif et l'application de ces lois aux évolutions du terrorisme. Ces lois font honneur à notre pays. Ne parlons donc pas de lois d'exception ou de lois liberticides, d'autant que la menace est toujours là.

L'unification de ces dispositifs est tout à fait nécessaire. Une telle évolution serait d'ailleurs de bonne administration et faciliterait l'exercice par la Commission nationale de contrôle des interceptions de sécurité de ses pleines prérogatives, ainsi que vous l'avez dit tout à l'heure. Nous devons y être attentifs.

Je ferai d'ailleurs moi-même des propositions en ce sens dans le cadre non seulement de l'élaboration, en cours, du Livre blanc sur la défense et la sécurité nationale, initiative lancée par le Chef de l'État, mais aussi de la mission d'information constituée par l'Assemblée nationale en vue d'évaluer le cadre juridique applicable à l'exercice des missions de renseignement.

Je ne vois aucun inconvénient à ce que cette unification intervienne le plus rapidement possible et j'œuvrerai dans ce but. »
http://www.senat.fr/seances/s201210/s20121016/s20121016013.html#section1195

[10] **Article 1er**
L'article 2 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication est complété par un alinéa ainsi rédigé :
« On entend par communication publique en ligne toute communication audiovisuelle transmise sur demande individuelle formulée par un procédé de télécommunication. »
http://www.assemblee-nationale.fr/12/projets/pl0528.asp

[11] Amendement déposé par
MM. HÉRISSON et SIDO
au nom de la commission des affaires économiques et du Plan

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

[12] « Le projet de loi relatif aux « communications électroniques et services de communication audiovisuelle » vise à transposer en droit national un ensemble de directives communautaires, communément désignées sous le nom de « paquet télécoms », issues de la consultation sur la « convergence » lancée en 1997 par la Commission européenne et finalement adoptées en mars 2002. »
http://www.senat.fr/dossier-legislatif/pjl03-215.html

[13] « AMENDEMENT
présenté par
MM. HÉRISSON et CÉSAR et Mme LAMURE
ARTICLE 13
Alinéa 9
Remplacer les mots :
du réseau
par les mots :
de l'opérateur

Objet

Ce projet de disposition concerne le recueil d'informations par les personnes habilitées aux finalités énumérées à l'article L. 241-2.
La méthode proposée pour permettre l'accès aux données sensibles, à savoir un raccordement direct aux réseaux des opérateurs, soulève de nombreuses difficultés de mise en œuvre car elle se distingue très nettement de celle habituellement utilisée et qui a pourtant fait ses preuves.
Par souci d'efficacité, de sécurité juridique et de limitation de l'impact sur les réseaux exploités par les opérateurs télécoms, il est préconisé de capitaliser sur des plateformes existantes : la plateforme GIC (Groupement Interministériel de Contrôle) / UCLAT (Unité de Coordination de Lutte Antiterroriste) et la plateforme nationale d'interception judiciaire (PNIJ), outil de centralisation et de mutualisation supervisé par le ministère de la justice et récemment mise en place.
Ceci passe donc par la sollicitation des experts accrédités chez les opérateurs télécoms permettant tout à la fois d'atteindre l'objectif de réactivité le plus fort tout en affectant le moins possible le fonctionnement des réseaux exploités par les opérateurs télécoms.
Toute prise directe sur les réseaux télécoms pourrait de surcroît faire courir des risques d'incidents techniques ou de dysfonctionnements opérationnels, avec des incidences non négligeables sur les services fournis aux clients et pour lesquels les opérateurs sont contraints à des exigences élevées de qualité de service.
S'il est légitime que les opérateurs contribuent encore davantage à la préservation des intérêts vitaux de la Nation par toute transmission diligente et accélérée de données sensibles qui transitent via leurs équipements, il reste préférable que les opérateurs télécoms gardent le contrôle des réseaux dont ils garantissent la sécurité et sont juridiquement responsables. »

[14] « La ministre a rapidement dû faire face aux interrogations sur la nouvelle loi, et a dû jouer l'apaisement :
« Il est normal d'effectuer une mise à jour technologique des outils à disposition de la police pour la lutte contre le terrorisme et le crime organisé. L'article 13 renforce en réalité le contrôle démocratique sur le renseignement. Surtout, il y aura par la suite un décret d'application qui précisera les modalités » de la fameuse interception.»

http://www.zdnet.fr/actualites/lpm-pour-fleur-pellerin-l-article-13-renforce-le-controle-democratique-39796285.htm

[15] « 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. »

[16] LOI n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle

Article 125

La loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications est ainsi modifiée :
1° Dans le titre et dans les dispositions de la loi, le mot : « télécommunications » est remplacé par les mots : « communications électroniques » ;
2° A l'article 11, le mot : « autorisés » est supprimé ;
3° Au premier alinéa de l'article 22, les mots : « ou l'organisme visé à l'article L. 35-4 du code des postes et télécommunications » sont supprimés.
http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000439399&categorieLien=id#JORFARTI000001286256