Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

LE PRESIDENT DU CONSEIL NATIONAL DU NUMERIQUE

Paris, le 12 juin 2015

Note à l'attention des membres du Conseil constitutionnel sur le projet de loi relatif au renseignement

Objet : Contribution du Conseil national du numérique à la réflexion du Conseil constitutionnel sur les enjeux techniques et économiques du projet de loi relatif au renseignement

Sommaire

1. L'impératif d'un contrôle effectif des activités de renseignement
1. 1. La nécessaire dimension technique du contrôle
1. 2. La nécessité pour la CNCTR de disposer de compétences de contrôle et d'audit renforcées
1. 3. Régime applicable à la surveillance internationale : un risque de brèche dans le contrôle de la CNCTR ?

2. Le dispositif de détection automatisée d'une menace terroriste : un outil à l'efficacité critiquée et au caractère attentatoire aux libertés fondamentales
2. 1. Un dispositif technique à l'efficacité limitée
2. 1. 1. Sur la question des "faux-positifs"
2. 1. 2. Sur la question des risques en termes de sécurité des réseaux
2. 2. Un dispositif particulièrement attentoire au droit fondamental au respect de la vie privée
2. 2. 1. La collecte de métadonnées n'est pas moins attentatoire aux libertés que la collecte des contenus
2. 2. 2. Une anonymisation complète des données est illusoire
2. 2. 3. Une nécessaire inspection en profondeur du trafic (deep packet inspection)
2. 3. Un modèle panoptique préjudiciable à la libre expression

3. Extension du périmètre du renseignement et risques économiques
3.1 Erosion de la confiance et fuite de la demande
3.2. Fuite de la demande et délocalisation de l'offre

4. Une extension problématique des finalités : surveillance indiscriminée et risques de police politique

5. Des régimes problématiques de conservation des données
5.1. Le régime dérogatoire de conservation des renseignements chiffrés : un risque de brèche pour les renseignements en clair y afférant
5.2. Un manque d'encadrement de la conservation des fichiers et des renseignements "raffinés"

CNNum
Conseil National du Numérique

BATIMENT ATRIUM – 5 PLACE DES VINS DE FRANCE 75572 PARIS CEDEX 12
TEL. 01 53 44 21 27 – MEL. INFO@CNNUMERIQUE.FR

1. L'impératif d'un contrôle effectif des activités de renseignement

II est impossible de faire abstraction des révélations d'Edward Snowden sur les pratiques de surveillance généralisée car celles-ci posent la question de la confiance. Le manque de pont entre la Nation et ses services de renseignement amène souvent à un climat de défiance, des réactions épidermiques et suspicieuses. Le chantier législatif devrait avoir pour but de développer la redevabilité (*accountability*) de la communauté du renseignement. Cette dernière doit communiquer et rendre des comptes au public sur son action. Dès lors, il est indispensable que le contrôleur joue un rôle de tiers de confiance aux fins de garantir la qualité démocratique de ses actions. Pour ce faire, la mise en place d'un organe dédié effectif, indépendant, autonome et compétent est fondamentale pour lutter contre les risques de dérive induits par une surveillance massive.

Pour l'heure, certaines évolutions apportées au projet de loi méritent d'être saluées. C'est le cas, notamment, pour ce qui concerne la centralisation des données, la CNCTR disposant à l'issue du débat parlementaire d'un accès non seulement « *permanent* » mais également « *direct* » aux éléments centralisés. Toutefois, il apparaît que certaines brèches subsistent, ce qui peut nourrir de sérieuses inquiétudes.

1. 1. La nécessaire dimension technique du contrôle

Les techniques informatiques, et notamment algorithmiques, nécessitent des compétences très spécifiques. A tel point que les informaticiens, « *codeurs* » et experts en algorithmes sont aujourd'hui ardemment recherchés par les entreprises. Il est par conséquent difficile - pour ne pas dire impossible - pour une personne non spécialiste d'appréhender les tenants et aboutissants d'un programme informatique, que ce soit dans ses implications techniques, juridiques ou politiques. Auditer un logiciel nécessite en effet d'assimiler des centaines de milliers de lignes de codes. Au regard de ces considérations, il est donc légitime de s'interroger sur les moyens accordés à la CNCTR quant à la qualité du contrôle qu'elle effectuera. Or, la composition actuelle de la CNCTR ne prévoit la présence que d'une seule personne spécialiste des réseaux et communications électroniques, nommée sur proposition de l'ARCEP, parmi les 9 membres qu'elle devrait comporter.

Un manque de compétence technique des personnes chargées du contrôle aboutirait à une incompréhension des enjeux, reléguant la future CNCTR à une simple « *commission tampon* ». L'exemple du contrôleur américain est à ce titre particulièrement éclairant. De 1979 à 2012, la FISA Court - l'équivalent américain de la CNCTR - a reçu 33 949 demandes de mandats et en

accepté 99,97%, soit 12 rejets en 33 ans[1]! Le Congrès dispose par ailleurs de deux commissions spécialisées aux pouvoirs étendus, entièrement dédiées au contrôle des services de renseignement. Pourtant, malgré l'existence de programmes de surveillance massive constituant une violation flagrante de la Constitution américaine, ces commissions parlementaires sont restées inertes depuis 2001.

1. 2. La nécessité pour la CNCTR de disposer de compétences de contrôle et d'audit renforcées

L'autorité de contrôle doit nécessairement disposer de compétences de contrôle et d'audit renforcés, à la mesure de l'extension du champ de compétence des services de renseignement. Pour le Commissaire aux droits de l'homme du Conseil de l'Europe, il incombe à la représentation nationale d'assurer le retour démocratique des activités de renseignement, en s'assurant que les lois nationales permettent un contrôle effectif des services, en allouant les ressources budgétaires nécessaires aux autorités de contrôle et en évaluant l'effectivité du contrôle de ces commissions *ad hoc*[2]. Pour le Commissaire, en effet, « *il est essentiel que les systèmes de contrôle soient périodiquement évalués pour déterminer s'ils possèdent les attributs nécessaires à leur effectivité. Cette évaluation peut être périodique ou ad hoc* »[3].

A titre de comparaison, le contrôleur britannique (*Intelligence Service Commissionner & Interception of Communication Commissionner*) dispose de véritables pouvoirs de contrôle des services : il surveille la conformité des perquisitions (y compris électroniques) et des missions de surveillance menées par les services ; il mène à discrétion des visites d'inspection dans les services ; il entend les agents de son choix et de différents grades au sein des équipes ; et tout membre des services de renseignement doit lui fournir les documents qu'il requiert, sans qu'aucune limite ne puisse lui être opposée. L'ISC comme l'IOCCO sont dotés d'une équipe compétente et spécialisé qui l'appuie dans ses missions et dans un travail de documentation. A l'inverse, le projet de loi sur le renseignement, s'il introduit un accès direct et permanent de la CNCTR aux renseignements collectés, ne lui accorde pas un droit d'audition et d'accès aux documents illimité.

1. 3. Régime applicable à la surveillance internationale : un risque de brèche dans le contrôle de la CNCTR ?

---

[1] Electronic Privacy Information Center, "Foreign Intelligence Surveillance Act Court Orders 1979-2014", disponible sur : https://epic.org/privacy/wiretap/stats/fisa_stats.html

[2] Conseil de l'Europe, Commissariat aux droits de l'homme, « *Positions on counter-terrorism and Human rights protection* », Strasbourg, 5 juin 2015, disponible sur : https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2757196&SecMode=1&DocId=2274090&Usage=2

[3] *Idem*.

Le texte prévoit que le renseignement à l'étranger fait l'objet de dispositions spécifiques. Il est notamment prévu à l'article L. 833-2-1 du futur CSI que, pour l'accomplissement de ses missions de contrôle, la CNTCR dispose d'un accès permanent et direct aux renseignements collectés, à l'exception de ceux mentionnés à l'article L. 854-1 qui sont issus de la surveillance et du contrôle des communications qui sont « *émises* ou *reçues à l'étranger* ». Il suffit donc d'un élément d'extranéité pour que le pouvoir d'audit de la CNCTR soit exclu.

Or d'un point de vue purement technique, une grande majorité des communications des ressortissants français peuvent être considérées comme étant « *émises ou reçues à l'étranger* ». Il suffit par exemple qu'une boite mail soit hébergée sur un serveur situé à l'étranger pour que les communications qui en émanent relèvent de cette catégorie. Ou encore qu'une personne choisisse de domicilier sa connexion à l'étranger en utilisant un Réseau privé virtuel (VPN). A ce titre, l'avis de l'ARCEP sur le projet de loi relatif au renseignement en date du 5 mars 2015 relevait à juste titre qu'il « *pourrait être délicat pour les opérateurs de déterminer de manière suffisamment certaine le régime dont relèvent les communications internationales émises ou reçues sur le territoire national* »[4].

Il est certes prévu à l'article L.854-1 que lorsque les correspondances interceptées renvoient à des numéros d'abonnement ou des identifiants techniques rattachables au territoire national, leur exploitation est opérée dans les mêmes conditions que pour les communications ayant fait l'objet d'une technique de renseignement sur le territoire national. Seulement, si la procédure d'exploitation est la même, la procédure de contrôle ne l'est pas, puisque les données recueillies ont été soustraites au contrôle *a priori* de la CNTCR, le retour au régime de droit commun n'étant opéré qu'après que l'interception a été effectuée. Ce dispositif risque donc de limiter le pouvoir de contrôle de la CNTCR pour ce qui constitue potentiellement la très grande majorité des communications des citoyens.

2. Le dispositif de détection automatisée d'une menace terroriste : un outil à l'efficacité critiquée et au caractère attentatoire aux libertés fondamentales

Le projet de loi sur le renseignement organise un double régime de captation, selon que la personne *suspecte* est identifiée ou non. L'article L. 851-3 du futur CSI prévoit tout d'abord, pour des personnes déjà identifiées et suspectées de préparer ou commettre un acte terroriste, un régime de collecte et de stockage « *des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques* ». Cette

[4] ARCEP, Avis n° 2015-0291 du 5 mars 2015 sur le projet de loi relatif au renseignement, disponible sur : http://www.arcep.fr/uploads/tx_gsavis/15-0291.pdf

disposition, qui instaure une surveillance ciblée sur un nombre déterminé d'individus, apparaît proportionnelle à l'objectif poursuivi de lutte contre le terrorisme.

A l'inverse, l'article L. 851-4 du futur CSI prévoit un régime spécifique d'exploitation massive « *des informations ou documents [...], y compris les données techniques [...] sur la seule base de traitement automatisés* », visant à « *détecter une menace terroriste* » sans permettre « *l'identification des personnes* ». Il s'agit des fameuses « *boîtes noires* », largement controversées. Ce mode de collecte des données confine à une forme de surveillance généralisée et indiscriminée des réseaux[5], pour une efficacité qui apparaît toute relative.

2. 1. Un dispositif technique à l'efficacité limitée

De façon imagée, les algorithmes sont souvent comparés aux recettes de cuisine : une série d'instructions et d'ingrédients précis aboutissent à un plat. L'analogie culinaire est pertinente, car si certaines recettes peuvent facilement être déduites de l'assiette posée devant soi, d'autres sont bien plus difficiles à déterminer - *a fortiori* à reproduire.

Un algorithme correspond ainsi à une suite d'opérations ou d'instructions, décrivant un calcul exécutable par une machine et visant à résoudre un problème ou un ensemble de problèmes. L'algorithme est dit *correct* lorsque, pour chaque instance du problème, il se termine en produisant la bonne sortie, *i.e.* qu'il résout le problème posé. L'algorithme correspond à un calcul mécanique. Il est incapable de « bon sens », ni de jugement personnel. Derrière chaque algorithme se trouve ainsi un humain. Si l'ordinateur exécute, c'est bien l'être humain qui définit et paramètre ce qu'il doit exécuter.

2. 1. 1. Sur la question des "*faux-positifs*"

A la lumière de ces considérations, l'efficacité du dispositif de détection automatisée d'une menace terroriste prévu par le projet de loi peut être interrogée. En l'état de l'art, les spécialistes sont unanimes : quand bien même le dispositif algorithmique en question serait extrêmement sophistiqué, il ne pourrait pas échapper à une quantité significative de « *faux positifs* », *i.e.* des individus identifiés comme potentiellement suspects et qui se révèleront hors de tout soupçon. Les professionnels de l'Institut national de recherche en informatique et en automatique (Inria) en font la démonstration :

> Supposons que l'on recherche des terroristes dans une population. Tout algorithme de détection a une marge d'erreur c'est à dire va identifier des personnes sans intention terroriste (des « faux-positifs »). Si la marge d'erreur est de 1%, ce qui est considéré à ce jour comme très faible, l'algorithme identifiera

[5] En effet pour de simples raisons de ressources humaines, une surveillance de masse ne peut être qu'automatique et algorithmique, quand bien même aucun humain ne « lirait » le contenu des communications.

quelques 600 000 personnes sur une population totale de 60 millions de personnes. Si le nombre de vrais terroristes est par exemple de 60, ces vrais terroristes ne représenteront que 0,01% de la population identifiée[6] [comme potentiellement suspecte].

En effet, les comportements « *terroristes* » ne présentent pas une fréquence suffisante pour permettre de nourrir une méthode automatisée. Ce phénomène, très connu, est lié à l'identification statistique d'évènements rares. De plus, les individus ciblés par ce dispositif adopteront un comportement visant à échapper aux modèles de comportements (*patterns*) paramétrés par l'algorithme puisqu'ils s'adapteront en permanence pour échapper à la détection. Dans un contexte de lutte anti-terroriste, le rapport du Commissaire aux droits de l'homme du Conseil de l'Europe remarque en outre que ces faux positifs pourraient déboucher sur des discriminations à grande échelle, fondées sur la race, le genre, la relation ou la nationalité[7].

Au vu des considérations qui précèdent, il semble à tout le moins malaisé de comparer, comme l'a fait le Gouvernement, ces méthodes de détection automatisées avec les traitements massifs de données des géants de l'Internet, opérés à des fins de ciblage publicitaire : non seulement ces derniers allouent à la recherche et au développement de leurs algorithmes des budgets astronomiques, mais ils utilisent des traces présentant une fréquence beaucoup plus importante - les habitudes de consommation : si les algorithmes d'Amazon sont doués pour recommander des livres qui plairont à ses clients, c'est en effet parce que le géant du net se fonde sur des millions d'objets achetés par le passé.

2. 1. 2. Sur la question des risques en termes de sécurité des réseaux

Dans son avis du 5 mars 2015, l'ARCEP relevait déjà que « *la mise en oeuvre de certaines techniques de recueil de renseignements serait susceptible d'avoir un impact sur l'intégrité et la disponibilité des réseaux ou sur la qualité des services de communications électroniques* »[8]. Le dispositif de traitement automatisé présente en outre des risques pour la sécurité des réseaux. Ainsi placés dans les réseaux des opérateurs et des hébergeurs, ces « *boîtes noires* » - classées secret-défense - ne pourront pas être contrôlées par les personnes qui les hébergent. Elles pourraient ainsi présenter des failles de sécurité potentiellement très critiques pour leurs réseaux, puisqu'il sera par définition impossible de les auditer.

---

[6] INRIA, Note interne du 30 avril 2015, « Elements d'analyse technique du projet de loi sur le renseignement », disponible sur : http://www.cil.cnrs.fr/CIL/IMG/pdf/265206918-Note-interne-de-l-Inria.pdf

[7] Conseil de l'Europe, Commissariat aux droits de l'homme, « *Positions on counter-terrorism and Human rights protection* », Strasbourg, 5 juin 2015, disponible sur : https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2757196&SecMode=1&DocId=2274090&Usage=2

[8] ARCEP, Avis n° 2015-0291 du 5 mars 2015 sur le projet de loi relatif au renseignement, disponible sur : http://www.arcep.fr/uploads/tx_gsavis/15-0291.pdf

Par ailleurs, les données récoltées ne pourront pas être analysées directement sur ces dispositifs, déjà fort occupés à exfiltrer les informations d'un trafic important. Les logiciels d'analyse devront pouvoir croiser les informations de différentes sources, émises à des instants *t* différents. Il sera donc nécessaire de stocker et d'agréger les données exfiltrées pour une analyse ultérieure, donc de les placer dans des bases de données qui seront, elles, centralisées.

2. 2. Un dispositif particulièrement attentoire au droit fondamental au respect de la vie privée

Le dispositif de détection automatisée d'une menace terroriste introduit un nouveau paradigme dans le renseignement : l'algorithme fait son entrée dans notre mode de gouvernance. Cela semble, à tout le moins, aller à rebours de la lettre et l'esprit de l'article 10 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifié par la loi du 6 août 2004, qui dispose qu'« *aucune décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité* ».

2. 2. 1. La collecte de métadonnées n'est pas moins attentatoire aux libertés que la collecte des contenus

Le projet de loi sur le renseignement prévoit plusieurs régimes de collecte, d'enregistrement et de stockage des données techniques de connexion (les métadonnées ou *metadata*). Une métadonnée est une donnée servant à définir ou décrire une autre données : il s'agit des informations qui décrivent *techniquement* une communication (« qui ? », « où ? » et « quand ? »). Elles s'opposent donc au *contenu* de cette communication (« quoi ? »). Un exemple type de métadonnée est la date associée à une photo, ou les coordonnées GPS du lieu où elle a été prise.

Contrairement à une croyance répandue, les données de connexion peuvent être extrêmement révélatrices, prises seules mais surtout lorsqu'elles sont agrégées. Comme le remarque la CNIL – les données collectées par l'algorithme ne sauraient constituer des éléments anonymes dans la mesure où les métadonnées sont indirectement ou directement identifiantes. Il est en effet très facile d'assurer l'identification d'un individu en combinant un petit nombre de traitements de données. A l'instar de nombreuses études[9], la Cour de justice de l'Union européenne l'a expliqué très clairement : « *ces données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la personne dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les*

[9] Par exemple : Jonathan Mayer, Patrick Mutchler, « MetaPhone: The Sensitivity of Telephone Metadata », 12 mars 2014, disponible sur : http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata

déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci »[10].

Les métadonnées sont en réalité souvent plus intéressantes que les contenus des communications eux-mêmes, car elles donnent les réponses aux questions les plus importantes sur nos habitudes, nos fréquentations, nos centres d'intérêts, nos religions (fréquentation régulière d'un lieu de culte), notre santé (appel d'un medecin spécialiste) et nos opinion. L'analyse des métadonnées (données de connexion) se prête plus aisément à une surveillance automatisée, générale ou exploratoire qu'une analyse des contenus qui, parce qu'elle suppose une étude en profondeur, est plutôt adaptée à un cadre d'enquête. C'est d'autant plus vrai à la lumière de la célèbre "*loi*" de Moore[11], qui prévoit l'augmentation exponentielle des capacités de stockages à prix constant, et donc le décuplement des capacités des services de renseignement à enregistrer ces données.

Partant, la *summa divisio* entre les données de connexion et les données de contenus n'a probablement pas la même portée qu'il y a quelques années, et sans doute l'ingérence dans la vie privée que constitue l'accès aux données de connexion devrait être réévaluée.

2. 2. 2. Une anonymisation complète des données est illusoire

Selon la définition proposée par l'Inria, « *l'anonymisation consiste à modifier un ensemble de données de manière à ce qu'on ne puisse pas identifier un ou plusieurs critères particuliers qui leur sont initialement attachés tels que l'identité de personnes, la localisation de faits, l'entité ayant recueilli les informations, etc* ».

Comme le note l'Institut, « *l'anonymisation est un problème de recherche largement ouvert et il n'existe pas aujourd'hui de technique d'anonymisation sûre* »[12]. Aucune technique d'anonymisation ne résiste actuellement de manière robuste au croisement des sources d'information : par exemple, note l'Inria, « *le croisement d'un fichier concernant, dans un hôpital, un ensemble de patients dont on a supprimé les informations nominatives (et donc a priori "*anonymes*") avec les informations temporelles ou de localisation de personnes accédant à l'hôpital permet très largement de désanonymiser ce fichier patient* ».

[10] CJUE, arrêt du 8 avril 2014 (C-293/12 et C-594/12)
[11] La « loi de Moore » a été exprimée en 1965 dans « Electronics Magazine » par Gordon Moore, ingénieur de Fairchild Semiconductor, un des trois fondateurs d'Intel. Constatant que la complexité des semiconducteurs proposés en entrée de gamme doublait tous les ans à coût constant depuis 1959, date de leur invention, il postulait la poursuite de cette croissance. Cette augmentation exponentielle fut rapidement nommée Loi de Moore.
[12] INRIA, Note interne du 30 avril 2015, « Elements d'analyse technique du projet de loi sur le renseignement », disponible sur : http://www.cil.cnrs.fr/CIL/IMG/pdf/265206918-Note-interne-de-l-Inria.pdf

2. 2. 3. Une nécessaire inspection en profondeur du trafic (*deep packet inspection*)

M. Bernard Cazeneuve a donné quelques exemples de l'utilisation qui pourra être faite du dispositif par les services de renseignement. Ces exemples sont éclairants car ils permettent de mieux appréhender le périmètre technique du dispositif. Selon le ministre de l'Interieur :

> L'algorithme permettrait de repérer les premières connexions à [une] vidéo [de décapitation], émanant de France. L'idée serait alors de repérer des Français complices de la publication de cette vidéo[13].

Afin d'identifier cette vidéo, les services de renseignement devront scruter le trafic Internet pour déterminer les URL, *i.e.* les adresses des vidéos. Par la même, ils devront s'intéresser au *contenu* des communications, car déterminer l'URL suppose une inspection en profondeur des communications électroniques - ce que l'on appelle le *deep packet inspection* (DPI). Le DPI reste en effet le seul type de techniques utilisable pour faire le tri entre les métadonnées ciblées par le texte et le reste du trafic. C'est aussi un moyen très controversé : il s'agit d'une technique utilisée par les gouvernements totalitaires pour surveiller leurs populations et pratiquer la censure généralisée.

2. 2. 4. Une protection illusoire des professions sensibles

Suite aux nombreuses critiques de la part de représentants de professions sensibles - tels que Reporters sans frontières ou encore le Syndicat de la magistrature - le Gouvernement a présenté en séance à l'Assemblée deux amendements (386 et 410) ne visant pas, selon ses termes « *à interdire la mise en œuvre de techniques de renseignement à leur encontre, mais à les encadrer* »[14]. L'amendement n°386 prévoit d'une part que l'ensemble des techniques de renseignement ne puisse être mis en œuvre « *à l'encontre d'un magistrat, un avocat, un parlementaire, ou un journaliste ou concerner leurs véhicules, bureaux ou domiciles* » uniquement sur autorisation du Premier ministre. Il prévoit d'autre part que contrairement aux retranscriptions des données des autres citoyens, celles qui concernent des individus exerçant des professions sensibles seront « *transmises à la Commission nationale de contrôle des techniques de renseignement qui veille au caractère nécessaire et proportionné des atteintes aux secrets attachés à l'exercice de ces activités professionnelles ou mandats qui y sont le cas échéant portées.* »

---

[13] « Loi sur le renseignement : la "boîte noire" reste obscure », LeMonde.fr, le 1er avril 2015, disponible sur : http://www.lemonde.fr/pixels/article/2015/04/01/loi-sur-le-renseignement-la-boite-noire-reste-obscure_4607264_4408996.html
[14] Assemblée nationale, amendement n°386 au projet de loi sur le renseignement, disponible sur : http://www.assemblee-nationale.fr/14/amendements/2697/AN/386.asp

L'amendement n°410 prévoit quant à lui l'exclusion de ces professions des procédures d'urgence. A l'occasion de ces dernières, il ne peut y avoir de pénétration domiciliaire ni de surveillance d'une profession sensible (magistrat, avocat, parlementaire et journaliste) sans avis préalable de la CNCTR et l'autorisation du Premier ministre[15]. Or, les dispositifs de traitement automatisés des communications prévus par l'article L. 851-4 CSI, déjà décrits précédemment dans cette note, sont basés sur la détection anonymisée de certains comportements de communication. Plus précisément, il s'agit par exemple de paramétrer par avance une liste de variables, mots clefs ou expressions, afin de pouvoir repérer les individus qui consulteraient certains contenus ou adopteraient des comportement, identifiés comme suspects.

Sachant d'une part que les personnes exerçant des professions sensibles utilisent le même réseau que l'ensemble de la population - réseau sur lequel ces dispositifs seront installées - et qu'il n'existe aucune base de données regroupant les données permettant d'identifier ces personnes, telles que les adresses IP (données qui par ailleurs peuvent tout à fait évoluer), il est techniquement impossible pour le logiciel responsable du traitement automatisé de ces données de connexion de faire une distinction entre ces professions et de potentiels terroristes, lorsqu'il détecte le comportement particulier qu'il est censé faire remonter.

La lecture d'une vidéo de propagande djihadiste entraînera donc la conservation, par l'algorithme à des fins d'analyse, des données de la personne qui la consulte, qu'il s'agisse d'un journaliste ou d'un potentiel terroriste. Cette conservation automatique pouvant toucher un ensemble vaste de données, y compris de métadonnées, il sera aisé, dans le cas d'un journaliste, d'en tirer des informations sur l'ensemble de ses sources et contacts. Cet état de fait technique pourrait entraîner de véritables menaces pour la garantie de la confidentialité des communications de ces professions sensibles, et donc du secret de l'enquête, de l'instruction, du délibéré, du secret applicable aux échanges relevant de l'exercice des droits de la défense, ou encore du secret des sources pour les journalistes.

2. 3. Un modèle panoptique préjudiciable à la libre expression

Comme le constatait David Kaye, Rapporteur spécial des Nations unies sur la promotion et la protection de la liberté d'opinion et d'expression, la vie privée protège la liberté d'expression[16]. C'est particulièrement le cas dans le monde numérique, où les informations sont stockées et les échanges, traçables : « *les technologies numériques offrent ainsi aux gouvernements et aux entreprises [...] une capacité sans précédent d'interférer avec les libertés d'expression et d'opinion* », note le rapporteur. Pour beaucoup le modèle de surveillance instauré par le projet de

[15] Assemblée nationale, amendement n°386 au projet de loi sur le renseignement, disponible sur : http://www.assemblee-nationale.fr/14/amendements/2697/AN/410.asp
[16] Human Rights Council, « Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression », David Kaye, 22 mai 2015

loi sur le renseignement tient du *panoptique*, cher à Jeremy Bentham. Dans *Panoptique*, l'auteur anglais détaille un nouveau principe d'architecture pour la construction de prisons :

> *L'ensemble de cet édifice est comme une ruche dont chaque cellule est visible d'un point central. L'inspecteur invisible lui-même règne comme un esprit ; mais cet esprit peut, au besoin, donner immédiatement la preuve d'une présence réelle. Cette maison de pénitence serait appelée panoptique, pour exprimer d'un seul mot son avantage essentiel, la faculté de voir d'un coup d'œil tout ce qui s'y passe.*

Dans une prison panoptique, les cellules, en cercle, contiennent les prisonniers. Le gardien, au centre, caché dans sa tour, peut surveiller tout le monde d'un coup d'oeil. Mieux, il peut s'absenter et les prisonniers, se croyant observés, continueront à se comporter comme s'ils étaient observés. Le projet de loi sur le renseignement, particulièrement dans ses aspects algorithmiques, semble ainsi proposer une mise à jour numérique du modèle panoptique, fondé sur les mêmes principes mais élaboré grâce aux technologies de l'information et de la communication. Ce panoptique numérique engendre un pouvoir de contrôle et de surveillance sans commune mesure avec le projet de Bentham : un algorithme, placé en coeur du réseau, pourra surveiller *en puissance* les comportements de 60 millions de Français pour en extraire les *anomalies*, les déviances mathématiques traduites des comportements suspects.

Comme dans le modèle de Bentham, cette architecture de la surveillance pourra avoir pour effet une normalisation des comportements. Le dispositif algorithmique aura lui-même une influence sur le comportement des individus, car le fait de se penser surveillé - alors même que ce n'est pas le cas - pousse à se conformer à une conduite prédéterminée et à l'auto-censure. Selon l'avocat Glenn Greenwald : « *La surveillance de masse crée une prison dans l'esprit qui est bien plus subtile mais bien plus efficace pour favoriser la conformité aux normes sociales, bien plus effective que la force physique ne pourra jamais l'être* »[17].

3. Extension du périmètre du renseignement et risques économiques

Parce qu'il aura pour conséquence une érosion de la confiance des utilisateurs, le projet de loi sur le renseignement présente des risques quant au développement de l'économie numérique. Par la même, il semble s'inscrire à rebours de l'ambition affichée par le Gouvernement de construire une véritable stratégie numérique, de concurrencer les géants américains de l'Internet et de relancer la croissance française.

3.1. Erosion de la confiance et fuite de la demande

[17] Glenn Greenwald, « L'importance de la vie privée », TED Talks [vidéo], disponible sur : http://www.ted.com/talks/glenn_greenwald_why_privacy_matters/transcript?language=fr

Dans un contexte post-Snowden où la protection de la vie privée et des données personnelles tend à devenir de plus en plus déterminante pour les consommateurs, ces dispositions menacent la confiance que pourront accorder les utilisateurs dans les produits et services numériques. En effet, la mise en place dans l'environnement numérique d'un système de surveillance généralisé est de nature à rendre illusoire la garantie d'une protection de la vie privée. Et donc de faire fuire des consommateurs inquiets qui, eux seuls, ont la possibilité de faire croître et pérenniser le potentiel de croissance de l'économie numérique par leur demande. À cet égard, suite aux révélations sur le programme PRISM, nombreux sont les exemples qui peuvent témoigner des repercussions négatives sur l'activité économique des entreprises visées de près ou de loin par le scandale.

Un rapport de la fondation *Information Technologie & Innovation Fundation* (ITIF) de 2013 mentionne que l'industrie américaine du cloud computing pourrait perdre de 22 milliards de dollars à 35 dollars sur les trois prochaines années en raison des révélations[18] d'Edward Snowden. L'étude du cabinet de conseil Forrester est quant à elle encore plus pessimiste, puisqu'elle annonce des pertes pouvant aller jusqu'à 180 milliards de dollars en 2016 pour l'industrie américaine en matière de cloud computing[19].

Bien que non expressément visée par les révélations, la société International Business Machines (IBM) a également annoncé des résultats fortement en baisse pour le troisième trimestre de 2013, notamment sur ses activités en Chine - comme la baisse de 22% de ses ventes de logiciel (software), ou celle de 40% pour le matériel (hardware) qui représente près de la moitié des revenus d'IBM. Persuadés que les pertes économiques de la société sont directement liées aux révélations, un groupe d'actionnaires de la société a intenté une classe action pour obtenir réparation du préjudice subi pour l'absence de redistribution de dividendes espérés[20].

Dans le même ordre d'idée, la société CISCO a signalé à la mi-novembre 2013 un ralentissement de 12% de ses ventes mondiales en raison de l'impact réputationnel des révélations de la NSA[21]. D'autant plus que les pertes réputationnelles et donc économiques subies par les acteurs numériques qui sont sous le spectre de la surveillance de masse sont et seront captées par des

[18] Information Technologie & Innovation Fundation, « How Much Will PRISM Cost the U.S. Cloud Computing Industry? », August 5, 2013, disponible en ligne sur : http://www.itif.org/publications/2013/08/05/how-much-will-prism-cost-us-cloud-computing-industry.
[19] Forrester Consulting, « The Cost of PRISM Will Be Larger Than ITIF Projects », August 14, 2013, disponible en ligne sur : http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects
[20] United States District Court Southern of New York, Class action : Complaint for violations of the Federal securities laws, Case 1:13-cv-08818-DL, December 12, 2013.
[21] Trevor Timm, How NSA Mass Surveillance is Hurting the US Economy, November 25,2013. Disponible sur https://www.eff.org/deeplinks/2013/11/how-nsa-mass-surveillance-hurting-us-economy

concurrents internationaux qui, eux y échappent - comme l'explique le technologue Edward W. Felten, ancien membre de la Federal Trade Commission :

> *« This (NSA revelation) is going to put US companies at a competitive disadvantage, because people will believe that U.S. companies lack the ability to protect their customers—and people will suspect that U.S. companies may feel compelled to lie to their customers about security »*[22].

Un état de fait partagé par un concurrent français, Stephan Ramoin, PDG de Gandi, qui précise :

> *« Je reçois tous les jours des clients américains ou asiatiques qui viennent chez nous, car nous ne sommes pas concernés par PRISM ou par la NSA. Si le texte passe tel quel, nous perdrons au moins 40% de notre chiffre d'affaires »*[23].

3.2. Fuite de la demande et délocalisation de l'offre

A l'heure où l'ambition affichée est de relancer la croissance économique en dotant notamment la France d'une stratégie numérique, et s'offrir ainsi l'opportunité de faire émerger des champions numériques nationaux dans une compétition mondiale, certaines dispositions du projet de loi pourraient asphyxier l'activité de certaines entreprises numériques françaises. En effet, en installant un climat de défiance sur le marché des biens et services numériques, ce projet de loi présente un risque de décrédibilisation des entreprises vis-à-vis de leurs clients, obligeant celles-ci à délocaliser progressivement leurs serveurs pour être à même de proposer des produits et services équivalents aux concurrents internationaux. Comme le relève la pétition « Ni Pigeons Ni Espions », initiée par plusieurs acteurs français du numérique et qui compte aujourd'hui 949 signataires : « *Mettre Internet massivement sous surveillance, c'est aussi sacrifier l'avenir numérique de la France, ses emplois et sa contribution à l'économie française* »[24].

Il existe en effet un risque de voir menacé le potentiel de croissance de notre économie numérique, ce qui ne manquera pas de déconstruire l'ambition numérique de la France en pérennisant notamment la position déjà dominante des acteurs américains sur le marché. Certains géants de l'Internet l'ont par ailleurs bien compris : la société Apple, par exemple, multiplie depuis plusieurs mois ses annonces en termes de sécurité, de vie privée et de chiffrement des données jusqu'à en faire une marque de fabrique[25] (en partie pour se racheter une conduite suite

---

[22] Edward W. FELTEN, NSA Apparently Undermining Standards, Security, Confidence, September 9, 2013. Disponible en ligne sur : https://freedom-to-tinker.com/blog/felten/nsa-apparently-undermining-standards-security-confidence/

[23] Sandrine Cassini, « Loi renseignement : le monde du numérique menace de délocaliser », 10 avril 2015. Disponible en ligne sur : http://www.lesechos.fr/tech-medias/hightech/0204293137141-projet-de-loi-sur-le-renseignement-les-hebergeurs-menacent-de-quitter-la-france-1110178.php?kmvD1xG2jjV9qGtt.99

[24] Pétition #NiPigeonsNiEspions : « Nous, acteurs du numérique, sommes contre la surveillance généralisée d'Internet ». Disponible en ligne sur : https://ni-pigeons-ni-espions.fr/fr/

[25] Voir : Numerama, « La nouvelle obsession d'Apple : protéger votre vie privée », le 9 Juin 2015 disponible sur : http://www.numerama.com/magazine/33336-la-nouvelle-obsession-d-apple-proteger-votre-vie-privee.html

aux révélations d'Edward Snowden sur la collaboration des géants du net avec la NSA). Parce qu'elles disposent par ailleurs d'une puissance financière inégalable, ces entreprises auront tôt fait de récupérer des parts importantes sur le marché mondial encore émergent de la *privacy*.

4. Une extension problématique des finalités : surveillance indiscriminée et risques de police politique

Il est regrettable que le débat autour du projet de loi ne se soit concentré qu'autour de la menace terroriste, alors même qu'il ne s'agit que d'une seule des sept finalités du renseignement élargies par le texte, et que les nouvelles dispositions de l'article L. 811-3 permettent de généraliser les méthodes extrêmement intrusives de la lutte contre le terrorisme à des domaines beaucoup plus vastes.

Il est notamment question de « *la prévention de la délinquance et de la criminalité organisée* », dont le régime est tentaculaire puisqu'il regroupe un nombre impressionnant d'infractions, sitôt qu'elles sont commises en « *bande organisée* » - une notion elle-même floue en droit pénal. Si cette finalité est présente depuis 1991 à l'article L. 242-1 du Code de la sécurité intérieure (CSI), force est de constater que le projet de loi sur le renseignement n'apporte pas d'éclaircissement sur le périmètre qu'elle recouvre, alors même qu'il étend les techniques de renseignement qu'elle justifie. Le projet de loi ne se contente pas d'accroître le caractère intrusif des techniques de renseignement pour des finalités pré-existantes, il élargit également le périmètre de ces finalités.

En ce sens, les « *intérêts économiques, industriels et scientifiques majeurs de la France* » peuvent justifier la surveillance d'un nombre extrêmement élevé d'individus : dans un contexte de tension économique importante et de rivalité internationale pour la compétitivité et l'attractivité, quelles recherches et quelles entreprises ne relèvent-elles pas d'un intérêt économique, industriel ou scientifique majeur de la France ?

« *Les intérêts majeurs de la politique étrangère de la France* » soulèvent le même type d'enjeux de définition ; avec quels arguments justifier que la surveillance de tel individu ne relève pas d'un intérêt majeur de la politique étrangère de la France ? Tout d'abord, la définition même de ces intérêts est stratégique, secrète et soumise à la discrétion de ceux qui sont en charge de mener cette politique : elle ne peut donc que difficilement faire l'objet d'une définition commune. Ensuite, la France, notamment du fait de sa place particulière dans le concert des nations, a des intérêts extrêmement variés et nombreux en termes de politique étrangère. Enfin, ces intérêts sont mouvants et peuvent évoluer rapidement au fil des événements, ce qui justifierait une surveillance suffisamment large pour pouvoir anticiper ces évolutions. Pour toutes ces raisons ce type de finalité peut justifier également une surveillance très étendue.

Le projet de loi autorise en outre les services à recourir aux techniques de surveillance pour des nouveaux motifs aux contours extrêmement flous, à savoir « *la prévention des atteintes à la forme républicaine des institutions, des violences collectives de nature à porter atteinte à la sécurité nationale...* ». L'objectif de lutter contre « *les atteintes à la forme républicaine des institutions* » est sans conteste un objectif louable. Mais ce n'est pas ici l'intention qui est remise en cause, mais bien le caractère opératoire de ce critère. Comment distinguer ce qui relève d'une remise en cause d'une institution en particulier ou du cadre institutionnel en général avec ce qui relève d'une atteinte à la République ?

De même, la définition des violences collectives de nature à porter atteinte à la sécurité nationale est potentiellement très fluctuante : le déroulement d'une manifestation par exemple ou l'émergence d'un mouvement politique localisé pourrait aisément remplir ces critères de définition. En effet, dans la mesure où les violences sont définies comme collectives, ne suffit-il pas qu'un acte de violence ait lieu, même isolément, pour que, comme par contagion, l'ensemble d'un mouvement collectif en soit responsable ? Quelques casseurs isolés, par exemple, et tous les participants à une manifestation pourraient ainsi être surveillés. Le risque d'apparition d'une police politique semble alors très important, surtout dans un contexte où des foyers locaux remettent en cause le pouvoir politique de manière radicale, et souvent insaisissable pour des moyens de police classiques, comme l'illustre le mouvement des Zones à défendre (ZAD).

5. Des régimes problématiques de conservation des données

5.1. Le régime dérogatoire de conservation des renseignements chiffrés : un risque de brèche pour les renseignements en clair y afférant

Le projet de loi sur le renseignement prévoit en son article 1er al. 58 (version de la commission des lois du Sénat) que concernant les « *renseignements qui sont chiffrés, le délai [de conservation des données] court à compter de leur déchiffrement* ». L'alinéa suivant précise qu'en cas de « *stricte nécessité et pour les seuls besoins de l'analyse technique, ceux des renseignements collectés qui contiennent des éléments de cyberattaque ou qui sont chiffrés, ainsi que les renseignements déchiffrés associés à ces derniers, peuvent être conservés au delà* » des durées légales de conservation des données, « *à l'exclusion de toute utilisation pour la surveillance des personnes concernées* ».

Le futur article L. 822-2 prévoit ainsi un régime dérogatoire de conservation des données pour les renseignements chiffrés. Cela ne semble pas porter une atteinte exceptionnelle au droit au respect de la vie privée compte tenu qu'avant leur déchiffrement, ces données sont inexploitables. Toutefois, il est plus surprenant que les données « *en clair* » associées à ces renseignements chiffrés soient soumises au même régime dérogatoire, alors même que celles-ci sont directement exploitables en l'état.

5.2. Un manque d'encadrement de la conservation des fichiers et des renseignements « *raffinés* »

Le projet de loi pose un nouveau régime de conservation des données récoltées par le biais des techniques de renseignement. Cependant, rien n'est prévu quant à la conservation - et la circulation au sein des services - des renseignements « *raffinés* » (notes diverses, etc) et des fichiers extraits de l'exploitation et l'analyse des données. En effet, le texte ne dit mot sur les fichiers de souveraineté, leur encadrement, la question de leur croisement intra-service, alors même que ces documents portent une atteinte équivalente au droit au respect de la vie privée et que le projet de loi est susceptible d'en accroître significativement le nombre et la sensibilité.

Benoit THIEULIN

Contacts :

Yann BONNET - Secrétaire général : yann.bonnet@cnnumerique.fr
Charly BERTHET - Rapporteur : charly.berthet@cnnumerique.fr

ANNEXES

ANNEXE 1. *L'exemple américain de la NSA*

Les programmes de surveillance massive mis en place par la National Security Agency (NSA) aux Etats-Unis apportent des éclairages pertinents sur l'efficacité de dispositifs de détection algorithmiques. Ces programmes sont aujourd'hui fortement remis en cause : plusieurs sections litigieuses du *Patriot Act* ont non seulement été jugées illégales par une Cour d'appel fédérale, mais elles ont également être révisées par une réforme souhaitée par la Maison Blanche, l'"*American Freedom Act*".

Il faut tout d'abord noter que l'efficacité de ces programmes de surveillance est très difficilement quantifiable, la mise en lumière d'une menace terroriste résultant, dans une majorité de cas, de la mise en oeuvre de différents outils de surveillance utilisés de façon complémentaire. Toutefois, divers rapports et témoignages permettent aujourd'hui de sérieusement remettre en cause l'efficacité des programmes se fondant sur une surveillance massive opérée outre-Atlantique.

Les différents dispositifs de surveillance de masse introduit à la suite des attentats du 11 septembre ont trouvé une justification dans le besoin pour les services de renseignement d'élargir le champ des informations à leur disposition. Selon le directeur de la CIA, Michael Hayden, ces informations, si elles avaient alors été disponible à temps, auraient permis de repérer et localiser les terroristes pour prévenir les attentats.

Ces suppositions ont aujourd'hui été largement remises en cause, notamment par un rapport de l'ensemble des inspections générales des services de renseignement américains, aujourd'hui déclassifié[26]. Il indique que les services de renseignement « *ont eu des difficultés à citer des cas spécifiques dans lesquels* [les programmes de surveillance] *ont directement contribué à des succès contre-terroristes* ». Le rapport conclut sur le rôle très limité de la collecte massive de données dans le succès des opérations de contre-terrorisme. Ces conclusions ont été complétées par des témoignages d'anciens agents du FBI, recueillis dans un article du NY Times[27], qui ont fait valoir la frustration des agents face au grand nombre de faux-positifs rencontrés, et donc le nombre de pistes non-concluantes poursuivies. Un ancien agent y affirme : « *Nous poursuivons un numéro, trouvons un professeur d'école avec aucune indication qu'il n'a jamais été impliqué dans le terrorisme international – dossier fermé.* [...] *Après avoir reçu des milliers de numéro et qu'aucun ne donne rien, vous ressentez de la frustration* ». Le même agent conclut : « *gaspiller les ressources du contre-terrorisme à la surveillance de professeurs d'écoles américains innocents rend l'Amérique moins libre et pas plus sûre.* »

[26] « Unclassified Report on the Resident's Surveillance Program », 10 July 2009 [fas.org/irp/eprint/psp.pdf]
[27] Lowell Bergman, et al, Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends, NY Times, Jan. 17, 2005 http://nytimes.com/2006/01/17/politics/17spy.html

Certes, ces témoignages anonymes sont à prendre avec mesure. La concordance avec les inquiétudes soulevées dans la note des chercheurs de l'INRIA, déjà citée précédemment, en ce qui concerne le nombre important de "faux positifs", est néanmoins frappante. Ils semblent attester d'une marge d'erreur incontournable qui implique non seulement un manque de précision, mais aussi la conservation des données d'un grand nombre d'innocents.

L'efficacité toute relative de la surveillance généralisée a enfin également été admise par les plus hauts cadres de la NSA elle-même, durant des auditions tenues suite aux révélations de l'affaire Snowden. En 2013, afin de justifier les programmes de surveillance alors hautement décriées, l'administration américaine a fait savoir que ces programmes ont contribué à déjouer 54 attentats. Lors d'une audition à la Commission juridique du Sénat américain, John Chris Inglis, directeur adjoint de la NSA, puis Keith Brian Alexander, directeur de l'agence jusqu'en 2014, sont pourtant largement revenu sur ces chiffres. Interrogé par le sénateur démocrate et sénateur du Vermont Patrick Joseph Leahy sur le rôle joué par la collecte massive de données pour empêcher ces 54 attentats, le directeur adjoint de la NSA explique tout d'abord que sur ces 54 attentats, seulement 13 concernaient le territoire américain, et admet ensuite qu'il n'existe réellement qu'un seul exemple dans lequel le programme de surveillance massive a été crucial pour déjouer un projet d'attentat, ajoutant qu'il s'agit de l'arrestation de Basaaly Moalin[28]. Lors de l'audition de l'ancien directeur de la NSA, Keith Brian Alexander, les chiffres avancés par John Chris Inglis sont confirmés *(voir les transcriptions des auditions en annexe)*.

Ces éléments permettent d'avancer une remise en cause de l'utilité de la surveillance de masse pour les services de renseignement, notamment en comparaison des techniques de surveillance ciblée et d'investigation traditionelle. L'agence de renseignement la plus puissante au monde, qui dispose sans doute des moyens techniques et financiers les plus importants et les plus sophistiqués, a été dans l'incapacité de traiter efficacement les vastes données détectées par les dispositifs de traitement automatisé des données de télécommunications. Cette inefficacité va de pair avec l'atteinte portée aux libertés fondamentales et la vie privée de milliers d'individus : c'est bien parce qu'elle collecte trop de données d'individus innocents qu'elle ne peut fonctionner efficacement.

[28] On sait aujourd'hui que ce dernier était un chauffeur de taxi américano-somalien, accusé d'avoir transféré 8500 dollars entre 2007 et 2008 à un membre du groupe Al Shabaab en Somalie. Source : http://www.arretsurimages.net/chroniques/2015-03-09/Basaaly-Moalin-le-seul-terroriste-demasque-par-la-surveillance-massive-de-la-NSA-id7546

ANNEXE 2. Extrait de l'audition de John Chris Inglis[29]

SEN. LEAHY: And Section 215 was critical to preventing 54 plots?
MR. INGLIS: No sir, and of those – and of those plots, 13 of those had a homeland nexus; the others had essentially plots that would have come to fruition in Europe, Asia, other places around the world. Of the 13 –
SEN. LEAHY: How many – how many of those 13 were plots to harm Americans?
MR. INGLIS: Of the 13 that would have had a homeland nexus, 12 of those, 215 made a contribution. The question you've asked, though, is more precise, in the sense of is there a but-for case to be made, that but for 215, those plots would have been disrupted, that's a – that's a very difficult question to answer, insomuch as that's not necessarily how these programs work. That's actually not how these programs work.
What happens is that you essentially have a range of tools at your disposal; one or more of these tools might tip you to a plot; others of these plots might then give you an exposure as to what the nature of that plot is. And finally, the exercise of multiple instruments of power, to include law enforcement power, ultimately completes the picture and allows you to interdict that plot.
SEN. LEAHY: Is there –
MR. INGLIS: There is an example amongst those 13 that comes close to a but-for example and that's the case of Basaaly Moalin.

ANNEXE 3. Extrait de l'audition de Keith Brian Alexander[30]

SEN. LEAHY: [...] Would you agree that the 54 cases that keep getting cited by the administration were not all plots, and out of the 54, only 13 had some nexus to the U.S. Would you agree with that, yes or no?
DIR. ALEXANDER: Yes.
SEN. LEAHY: OK. In our last hearing, Deputy Director Inglis' testimony stated that there's only really one example of a case where, but for the use of Section 215, bulk phone records collection, terrorist activity was stopped. Is Mr. Inglis right?
DIR. ALEXANDER: He's right. I believe he said two, Chairman; I may have that wrong, but I think he said two, and I would like to point out that it could only have applied in 13 cases because of the 54 terrorist plots or events, only 13 occurred in the U.S.

[29] Disponible sur : http://icontherecord.tumblr.com/post/57811913209/hearing-of-the-senate-judiciary-committee-on
[30] Disponible sur : http://www.dailykos.com/story/2013/10/04/1243770/-NSA-Dir-Gen-Alexander-Admits-Gov-t-Lied-About-54-Plots-Thwarted-By-Surveillance