Communication de données aux services de renseignement et vie privée

publié le **26/12/2013**, vu **5501 fois**, Auteur : IPNESS

Suite à l'affaire « Snowden » révélant la main mise des Etats-Unis sur les données du réseau à des fins de surveillance, plusieurs pays européens dont la France et la Belgique ont largement renforcé les pouvoirs de leurs services de renseignement en ce qui concerne la communication des données détenues par les opérateurs Internet.Ces lois sont susceptibles de porter une atteinte disproportionnée à la vie privée des citoyens et de faire peser une trop grande contrainte sur les opérateurs.

La

La communication de ces données est encadrée par la directive « conservation des données ». En France, la loi de programmation militaire promulguée le 19 décembre 2013[1] **(I)** et en Belgique la loi du 30 juillet 2013 **(II)** respectent et transposent cette directive qui laisse une grande liberté de transposition aux Etats-membres. Trop grande ?

Déjà, la directive est accusée de porter elle-même atteinte à la vie privée de façon disproportionnée en ce qu'elle n'apporte aucune garantie aux citoyens. Elle est actuellement remise en cause devant la CJUE. Une évolution européenne est donc susceptible de provoquer la révision des lois de transposition au regard du droit à la vie privée en apportant des garanties supplémentaires aux citoyens **(III)**.

Enfin et dans un mouvement plus global, l'Europe doit faire face au gouvernement américain pour protéger les données des citoyens **(IV)**. Un projet de règlement et de directive sont sur la table des négociations et visent notamment à pénaliser fortement les entreprises américaines qui ne se plieraient pas aux standards européens en matière de protection des données personnelles.

1. **LA REFORME CONTROVERSEE DU REGIME DE COMMUNICATION DES DONNEES DE CONNEXION EN FRANCE**

L'article 20 de la loi sur de programmation militaire (LPM) permet l'accès des services de renseignements aux données de connexion conservées par les opérateurs de communications électroniques et hébergeurs de contenus ayant l'obligation de les conserver[2].

Le régime relatif à la demande de données de connexion était jusqu'alors prévu par l'article L. 34-1-1 du code des postes et des télécommunications électroniques[3] permettant aux agents individuellement désignés et individuellement habilités des services de la police et de la gendarmerie nationale, d'exiger des opérateurs de communications électroniques la transmission des « *données conservées et traitées par ces derniers* » pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales et dans le cadre de la prévention des actes de terrorisme.

Une réforme législative se devait de clarifier le régime juridique de la géolocalisation en temps réel

au regard de la jurisprudence récente de la Cour européenne des droits de l'homme d'une part exigeant une base légale « *suffisamment précise* » et de la Chambre criminelle de la Cour de cassation d'autre part exigeant de surcroît un contrôle préalable de l'autorité judicaire[4].

L'article 20 de la LPM va plus loin et abroge l'article L.34-1-1 du code des postes et des télécommunications électroniques. Il propose désormais un seul régime applicable aux demandes de données de connexion y compris de géolocalisation en temps réel dans un chapitre VI intitulé « *Accès administratif aux données de connexion* ». Son régime est calqué sur celui des « *interceptions de sécurité* » dites écoutes administratives[5] et ne vise plus seulement des données mais aussi des « *informations ou documents* » (contenu), pour des finalités plus vastes au bénéfice de l'ensemble des services de renseignement.

Données concernées Les données concernées sont les *« informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications »* (futur article L.246-1 du code de la sécurité intérieure).

Comme l'a rappelé récemment la CNIL en séance plénière, la notion d' « *information ou document* » est bien trop vaste car elle englobe les données portant sur le contenu et plus seulement les données techniques auxquelles il est ensuite fait référence dans le texte. Cette notion est donc la plus à même de constituer une atteinte disproportionnée au droit à la vie privée.

Finalités Ces données de connexions peuvent être demandées « *pour les finalités énumérées à l'article L. 241?2 du code de la sécurité intérieure* » à savoir « *la recherche de renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupement dissous**[6]*** » (futur article L.246-1 du code de la sécurité intérieure).

Ce faisant, le projet de loi étend largement les motifs pour lesquels les données de connexion pourront être demandées.

Modalités particulières Les informations où documents 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* ». Si cette disposition vise l'encadrement spécial de la géolocalisation en temps réel, elle permet surtout aux agents de ne pas passer à chaque fois par un intermédiaire mais d'être connecté en temps réel sur le réseau de l'opérateur.

Qui demande ? Les personnes pouvant faire la demande sont élargies aux agents « *individuellement désignés et dûment habilités des services relevant des ministres chargés de la sécurité intérieure, de la défense* » mais aussi « *de l'économie et du budget* », chargés des missions prévues à l'article L. 241?2. La compétence ainsi confiée au ministère de l'économie et du budget semble viser la répression financière de la criminalité et/ou la répression de la criminalité financière.

Exclusion du contrôle a priori Les détracteurs de l'article 20 s'insurgent contre l'éviction du contrôle *a priori* de la mesure par le juge judiciaire qui est pourtant le gardien des libertés fondamentales selon l'article 66 de la Constitution. En effet le projet de LPM ne soumet pas les demandes à l'autorisation et au contrôle préalable de l'autorité judiciaire, alors que cette garantie avait été apportée par la Cour de cassation pour ces données de géolocalisation « *dynamique* »[7]

compte tenu de la « *gravité* » de l'ingérence opérée dans la vie privée.

Garanties Il encadre néanmoins, en l'état et selon le rapport du sénat[8], la mesure de plusieurs garanties jugées plus restrictives que celles prévues jusqu'alors par le code des postes et des communications électroniques:

- la décision est prise par une personnalité qualifiée placée auprès du premier ministre et désignée par la CNCIS[9], personnalité qui pourra néanmoins faire désigner des adjoints dans les mêmes conditions pour la suppléer ;
- la demande des agents désignés et habilités doit être motivée ;
- la CNCIS se voit communiquer les décisions accompagnées de leurs motifs dans les 48 heures et devra déclencher un contrôle a posteriori de la légalité de la mesure par la CNCIS dans les 7 jours si elle estime que la décision contrevient au dispositif légal mis en place ;
- la CNCIS aura un accès permanent aux dispositifs mis en place aux fins de contrôle et pourra adresser un recommandation aux Premier ministre sous 15 jours pour qu'il y soit mis fin.
- la mesure doit être limitée à 30 jours mais peut être renouvelée dans les mêmes conditions de forme et de durée.

Le projet de LPM prévoit en outre un contrôle de la CNIL[10] sur les décrets d'application de la loi nouvelle. Elle devra préciser « *notamment la procédure de suivi des demandes et les conditions et durée de conservation des informations ou documents transmis* » (article L.246-4 du projet de loi).

La CNIL a pourtant fait part de son mécontentement à travers deux communiqués[11] et souhaite à l'avenir être consultée sur tous les projets de lois concernant les données personnelles.

Malgré un encadrement fort des mesures de surveillance sollicitées, la mise en place d'un contrôle *a postériori* est susceptible de renforcer considérablement les obligations des hébergeurs et FAI en matière de communication des données et informations sur leurs clients.

La loi relative à la confiance dans l'économie numérique[12] encadre strictement le régime des données pouvant être obtenues auprès des hébergeurs qu'elle limite à celles « *de nature à permettre l'identification quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires* ». Un décret en date du 25 février 2011[13] précise qu'il s'agit de données purement techniques qui ne portent en aucun cas sur le contenu stocké par l'hébergeur (l'adresse IP de connexion, le nom d'utilisateur, la date et heure de l'opération sur le contenu).

Le projet de LPM vise quant à lui toute « information ou document » stockés par les hébergeurs (contenu). Les principaux acteurs du numérique en France qualifient de « *liberticide* » le projet de loi car il permet aux agents habilités et désignés d'accéder sans contrôle préalable à l'ensemble des données et informations conservées par un hébergeur, par exemple à l'espace dématérialisé (« cloud ») d'un client.

Il sera souligné *a contrario* que les finalités de la demande restent en grande partie limitées, font l'objet du contrôle de la CNCIS susvisé et que le juge exerce un contrôle a posteriori de la mesure.

Néanmoins certaines finalités restent floues et extensibles, par exemple *« la sauvegarde des éléments essentiels du potentiel scientifique de la France ».* Concrètement, une telle finalité dont on comprend l'enjeu en termes de contre-espionnage industriel, n'est-elle pas aussi le moyen pour les autorités administratives de se procurer des documents sensibles sachant qu'un contrôle de la CNCIS dans les 9 jours ne permettrait pas de rétroagir efficacement sur la potentielle fuite de documents sensibles ? En cela les acteurs concernés sont donc fondés à s'interroger sur l'impact

que la mesure aura concrètement et psychologiquement sur leurs clients.

Facteur de compétitivité, les entreprises française pouvaient se targuer de ne pas voir leurs données et celles de leur clients susceptibles de faire l'objet d'un contrôle gouvernemental comparable à celui qu'ont connus les géants du web outre-Atlantique et révélé par les affaires des écoutes de la NSA à travers le programme PRISM. L'ensemble des organisations professionnelles concernées par la mesure s'indignent, parmi elles, L'**Association des Services Internet Communautaires** (ASIC) qui défend notamment les intérêts des groupes comme Facebook, Deezer et Dailymotion, l'**IAB France et** branche française de l'Interactive Advertising Bureau qui fédère les acteurs de la publicité en ligne, le MEDEF et la **fédération SYNTEC**, qui regroupe 80 000 entreprises du secteur du numérique et de l'IT et le **Conseil National du Numérique**.

« *Patience et longueur de temps font plus que force ni que rage*[14] », il faudra attendre l'adoption de la loi puis de ses décrets d'application pour prendre réellement l'ampleur de ce projet de loi et des garanties qui entourent sa mise en œuvre, sachant que la CNIL et le conseil constitutionnel se prononcerons certainement.

2. **UNE VOIE SUIVIE PAR DE NOMBREUX ETATS-MEMBRES : L'EXEMPLE DE NOS VOISINS BELGES**

En Belgique, la loi du 30 juillet 2013 portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90 *decies* du Code d'instruction criminelle transpose en droit Belge les directives européennes de 2002 et 2006 sur la conservation des données[15].

L'article 126§1 de la loi du 13 juin 2005 impose aux opérateurs de la téléphonie et de l'internet la conservation des données techniques qu'ils traitent pendant un an : « *les fournisseurs au public de services de téléphonie fixe, de téléphonie mobile, d'accès à l'internet, de courrier électronique par internet et de téléphonie par internet, ainsi que les fournisseurs des réseaux publics de communications électroniques sous-jacents, conservent les données de trafic, les données de localisation, les données d'identification d'utilisateurs finals, les données d'identification du service de communications électroniques utilisé et les données d'identification de l'équipement terminal qui est présumé avoir été utilisé, qui sont générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés* ».

Cet article ne s'applique pas au contenu mais au contenant, elle impose la conservation des données techniques y compris des données de « localisation ».

Tout comme la LPM en France, cette loi est remise en cause en ce qu'elle permet aux services de renseignement Belges d'obtenir la communication de telles données pour des finalités larges et floues, en particulier pour « *la recherche, l'analyse et le traitement du renseignement relatif à toute menace contre la pérennité de l'ordre démocratique et constitutionnel ainsi que contre le potentiel scientifique et économique du pays et (d')en informer le gouvernement*[16]. ».

De surcroît, la loi permet le recueil de ces données pour la poursuite des *« infractions graves »*, finalité disproportionnée au regard des nécessités d'une société démocratique selon la ligue des droits de l'homme, l'ordre des avocats et l'association des journalistes professionnels Belges[17].

La loi Belge à suscité une levée de bouclier relativement grande en Belgique, notamment de la part de l'ordre des avocats. En revanche et en France, l'article 20 de la LPM qui peut paraître plus liberticide n'a pas suscité un émoi supérieur.

3. **LA DIRECTIVE "CONSERVATION DES DONNEES" EST SUCEPTIBLE DE PORTER**

DIRECTEMENT ATTEINTE AUX LIBERTES FONDAMENTALES.

Les garanties apportées à la transposition de la directive « conservation des données » sont susceptibles d'évoluer sous l'égide de la CJUE et de la commission européenne, notamment en ce qui concerne les finalités et durées de conservation des données.

Le rapport d'évaluation de la directive sur la conservation des données[18] préconisait déjà en 2011 de garantir la proportionnalité dans le processus intégré de stockage, d'extraction et d'utilisation des données, en réalisant d'abord une étude d'impact sur « *les conséquences d'une réglementation plus stricte du stockage, de l'accès et de l'utilisation des données de trafic sur l'efficacité et l'efficience du système de justice pénale et des services répressifs, sur la vie privée et sur les coûts pour l'administration publique et les opérateurs* ».

Cette étude doit porter notamment sur : *la cohérence entre la limitation des finalités de la conservation des données et les types d'infractions pénales pour lesquels l'accès aux données conservées et leur utilisation peuvent être autorisés ; l'harmonisation, et éventuellement la réduction des durées de conservation obligatoire des données ; un contrôle indépendant des demandes d'accès et du régime général d'accès et de conservation des données appliqué dans tous les États membres ; la limitation des autorités autorisées à accéder aux données ; la réduction des catégories de données à conserver*.

L'objectif de cette étude est de proposer un nouveau projet de révision du cadre actuel de la conservation des données respectant le principe de proportionnalité et comblant les lacunes d'une actuelle transposition inégale (durée de conservation, finalités, autorités habilitées à demander les données etc.) dans les 28 pays de l'UE, créatrice d'une véritable distorsion de concurrence entre les opérateurs.

Les cours constitutionnelles roumaine, allemande et tchèque ont annulé, respectivement en octobre 2009, mars 2010 et mars 2011, les lois transposant la directive en droit interne au motif qu'elles étaient inconstitutionnelles.

Dans un arrêt du 5 mai 2010, la Haute Cour irlandaise a décidé de poser une question préjudicielle sur la directive « *conservation des données* » à la CJUE afin de savoir si elle viole, ou non, les droits fondamentaux protégés par les traités de l'UE, la CEDH et la Charte des droits fondamentaux. Une question similaire de la Cour suprême Autrichienne y a été jointe[19].

Dans ses conclusions[20], l'avocat général soulève l'ingérence particulièrement caractérisée dans le droit au respect de la vie privée de l'obligation de collecte et conservation des données créant « *les conditions d'une surveillance qui, pour ne s'exercer que rétrospectivement à l'occasion de leur exploitation, menace néanmoins de manière permanente, pendant toute la durée de leur conservation, le droit des citoyens de l'Union au secret de leur vie privée* ». Il en conclut que la durée de conservation fixée à deux maximum est disproportionnée au regard des articles 7 et 52§1 de la Charte des droits fondamentaux de l'UE.

Il ajoute qu' « *il appartenait au législateur de l'Union de définir les principes fondamentaux qui devaient régir la définition des garanties minimales encadrant l'accès aux données collectées et conservées et leur exploitation* » puisque il est à l'origine de l'ingérence, parmi lesquelles et sans exhaustivité :

- la description des activités criminelles susceptibles de justifier l'accès des autorités nationales compétentes aux données collectées et conservées incorporant un degré de précision allant au-delà de celle d'«*infractions graves*» ;
- l'autorisation d'accès aux données collectées et conservées, en limitant celui-ci si ce n'est

aux seules autorités judiciaires, à tout le moins à des autorités indépendantes ;
- l'obligation, pour les autorités autorisées à accéder aux données, d'une part, de les effacer une fois leur utilité épuisée et, d'autre part, d'informer les personnes concernées dudit accès, à tout le moins a posteriori.

La décision de la CJUE suit généralement les conclusions de l'avocat général, en revanche elle pourrait comme le préconise ce dernier, imposer aux états membres de se conformer à ces exigences dans un temps raisonnable tout en poussant la commission à réviser la directive « *communication et vie privée* » rapidement.

Ainsi la transposition trop audacieuse de ses dispositions par les 28 pourrait connaître un recul et se voir apporter plus de garanties, notamment en ce qui concerne la France et la Belgique au regard des larges finalités pour lesquelles les données peuvent être conservée.

4. **LETHARGIE DE LA COUR SUPREME AMERICAINE ET REACTION EUROPEENE**

Outre atlantique, la conservation des données sur les citoyens non-Américains a été rendue possible par le *Foreign Intelligence Surveillance Act (FISA)* permettant aux Directeur National de l'Intelligence et procureurs généraux, depuis 2008, d'autoriser la collecte d'information sur les non-Américains supposés situés en dehors du territoire américain sans qu'il soit nécessaire d'obtenir un mandat, avec l'autorisation de la *Foreign Surveillance Intelligence Court* (FISC). Plusieurs recours ont été formés contre les dispositions du FISA permettant une telle surveillance, sans succès à ce jour.

Plusieurs associations arguaient au soutient de leur recours devant la Cour suprême d'une violation du quatrième amendement (droit à la vie privée) en démontrant que leurs correspondants étaient des cibles vraisemblables des interceptions ou surveillances opérées dans le cadre du dispositif légal, incluant une forte probabilité que ces mesures prise en application du FISA les touchent et donc leur porte un préjudice.

Le 26 février 2013, la Cour suprême des Etats-Unis rendait un arrêt[21] validant de ces interceptions au motif que l'existence d'un préjudice doit résulter d'une réelle menace et qu'une simple probabilité que des données recueillies, lors d'écoutes téléphoniques soient utilisées par la suite ne suffit pas (Vous êtes peut-être secrètement sous surveillance, mais vous ne pouvez le prouver).

Le 6 juin, *Le Guardian* et le *Washington Post* mettaient à jour le programme PRISM qui permet entre autre l'interception de « *données copiées depuis des réseaux publics ou privés vers les serveurs de la NSA, à partir des points d'atterrissement des câbles de fibre optique et des centres de commutation des données de l'internet entre les grands fournisseurs d'accès; cette interception de données est basée sur des accords négociés avec les opérateurs de ces réseaux (ou sur des injonctions judiciaires; ces interceptions ont sans doute également été opérées directement au niveau des câbles sous-marins lorsque c'était nécessaire)****[22]*** ». Le programme concerne les géants de l'Internet tels qu'Apple, Google, Microsoft, Verizon qui avouent petit à petit être concernés.

Le 18 novembre et après ces révélations, la Cour suprême rejetait sans commentaire le recours de L'*Electronic Privacy Information Center* selon lequel la FISC[23] avait largement outrepassée ses pouvoirs en interprétant le FISA[24] de telle manière qu'il permettait de demander à un opérateur tel que Verizon (un des plus grands opérateurs de télécommunications aux Etats-Unis et dans le monde) de lui communiquer toute ses données de télécommunication.

Face au manque de considération des Autorités de renseignement et des juridictions Américaines,

le salut pourrait venir de l'Europe.

Un rapport du Parlement Européen recommande ainsi de nombreuse mesures stratégiques ayant *a minima* pour effet de rentre le Cloud européen plus attractif que les services Américains actuels [25].

Il est ainsi recommandé de faire afficher par les sites américains un message informant les clients européens "*que leurs données pourront faire l'objet d'une surveillance (au titre de l'article 702 de la FISA) par le gouvernement des États-Unis à toutes fins utiles à la politique étrangère des États-Unis*".

Le rapport suggère aussi et surtout d'annuler ou de renégocier les accords Europe/USA actuels, qui sont facilement contournés, et d'interdire strictement la communication de données européennes aux autorités américaines sans qu'un régulateur européen ait donné son accord préalable.

Le rapport ensuite préconise d'étudier le rétablissement de « *l'article 42* » du projet de nouveau règlement Européen abandonné sous la pression des lobbies Américains (selon la numérotation d'un projet de règlement divulgué deux mois avant la version finale) souhaitant interdire aux pays tiers (comme les États-Unis et tout autre État non membre de l'UE) d'accéder aux données personnelles des citoyens de l'UE à la demande d'une cour ou d'une autorité administrative extérieure à l'UE sans y avoir été préalablement autorisés par une autorité européenne de protection des données.

Cet article a été décrit comme la « clause anti-FISA ». Un tel article pourrait ne pas trouver à s'appliquer par les entreprises Américaines qui rétorquent pouvoir être accusées d'espionnage en suivant cette disposition. Le projet de règlement[26] prévoit néanmoins en l'état une amende pouvant aller jusqu'à 100.000.000 € où 5% du chiffre d'affaire annuel de l'entreprise afin de faire pression sur les entreprises Américaines proposant des services en Europe, en cas de violation de la nouvelle règlementation sur la protection des données personnelles.

Enfin, ce rapport préconise des mesures d'incitation et de protection pour les Wistleblowers[27] et une réforme de la gouvernance au sein du G29.

5. **OBSERVATION**

Notre attention se portera particulièrement sur :

- La publication des décrets d'application de l'article 20 de la LPM, et leur contrôle par la CNIL ainsi que les QPC susceptibles d'être formées contre le texte ;
- Les projets de directives et de règlement européen sur la protection des données personnelles ;
- L'arrêt de la CJUE à intervenir dans l'affaire Digital Rights Ireland c/ Seitlinger e.a. ;
- Les nombreux recours pendants devant la Cour suprême Américaine.

[1] Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale

[2] Les opérateurs de communications électroniques sont tenus de conserver ces données en vertu de l'article L.34-1 du code des postes et communications électroniques ; les hébergeurs et

FAI en vertu de l'article 6 de la loi du 21 juin 2004, loi pour la confiance dans l'économie numérique.

[3] Introduit par l'article 6 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.

[4] Crim. 22 octobre 2013, n° 13-81945 et n° 13-81949 ; ce faisant, la Chambre criminelle allait bien plus loin que la Cour européenne des droits de l'homme qui n'exigeait qu'un possible contrôle a postériori des mesures ; Gaz.pal. n°319 « Géolocalisation dynamique : le zèle de la Cour de cassation », note sous Cass.crim., 22 oct. 2013 par O. Bachelet ; Gaz.pal. n°305 à 309 « Géolocalisation : l'autorisation donnée par un magistrat du parquet est contraire à la Convention européenne des droits de l'hommes» note sous les mêmes arrêts par L. Robert.

[5] Régime institué par la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques aux articles L.241-1 à L.245-3 du code de la sécurité intérieure.

[6] Article L.241-2 du code de la sécurité intérieure.

[7] Crim. 22 octobre 2013, n° 13-81945 et n° 13-81949

[8] Rapport n° 195 (2013-2014) de M. Jean-Louis CARRÈRE, fait au nom de la commission des affaires étrangères, de la défense et des forces armées, déposé le 4 décembre 2013

[9] Commission nationale de contrôle des interceptions de sécurité

[10] Commission informatique et libertés.

[11] Communiqués des 26 novembre et 19 décembre 2013

[12] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

[13] 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.

[14] « Le lion et le rat », Jean de la Fontaine.

[15] transpose partiellement en droit belge la Directive 2006/24/CE sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la Directive 2002/58/CE (directive ?conservation de données?) et l'article 15.1 de la Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans

le secteur des communications électroniques

[16] L'aticle 126 §2 d) de la loi renvoie à l'accomplissement des missions de renseignement en ayant recours aux méthodes de collectes de données visées aux articles 18/7 et 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, dispositions qui visent cette finalité large.

[17] Ligue des Droits de l'Homme/Liga voor mensenrechten ; Avocats.be/Association des journalistes professionnels (AJP) ; Orde van Vlaamse Balies COMMUNIQUE DE PRESSE – 31 mai 2013 « Transposition de la directive européenne sur la conservation des données : un danger pour la vie privée et la démocratie.

[18] RAPPORT DE LA COMMISSION AU CONSEIL ET AU PARLEMENT EUROPÉEN ; Rapport d'évaluation concernant la directive sur la conservation des données (directive 2006/24/CE) du 4 avril 2011.

[19] CJUE aff. Jointes C-293/12 et C-594/12 Digital Rights Ireland ; Seitlinger e.a.

[20] Conclusions de l'avocat général M. Pedro Cruz Villalón présentées le 12 décembre 2013

[21] Supreme court of the united states ; clapper, director of national intelligence, et al. v. amnesty international usa et al. certiorari to the united states court of appeals for the second circuit no. 11–1025. argued october 29, 2012—decided february 26, 2013

[22] Rapport du Parlement Européen « Les programmes de surveillance des Etats-Unis et leurs effets sur les droits fondamentaux des citoyens de l'UE », DGPI, Dept. Thém. C

[23] *Foreign Surveillance Intelligence Court*

[24] *Foreign Intelligence Surveillance Act (et particulièrement l'article 1881a de la FISA)*

[25] Rapport du Parlement Européen « Les programmes de surveillance des Etats-Unis et leurs effets sur les droits fondamentaux des citoyens de l'UE », DGPI, Dept. Thém. C.

[26]Le 22 octobre 2013, la commission LIBE du Parlement européen a adopté de nouvelles propositions de règlement et de directive (IP/12/46 et IP/13/57) sous l'influence des différentes affaires concernant les écoutes téléphoniques de la NSA et pour mettre fin à un lobbying *« excessif et contre-productif »* comme l'a rappelé Viviane Reding, Vice-présidente à la commission Européenne.

[27] Les "dénonciateurs" comme Edward Snowden