

CONSEIL D'ETAT

SECTION DU CONTENTIEUX

QUESTION PRIORITAIRE DE CONSTITUTIONNALITE

Tendant à faire constater qu'en édictant les dispositions des articles L. 246-1, L. 246-2, L. 246-3, L. 246-4 et L. 246-5 du code de la sécurité intérieure, le législateur a méconnu sa propre compétence en affectant des droits et libertés que la Constitution garantit, notamment le droit au respect de la vie privée et la liberté de communication, en ce qu'il s'est abstenu, d'une part, de définir les notions d' « *informations ou documents* » et de « *sollicitation du réseau* » prévues respectivement par les dispositions des articles L. 246-1 et L. 246-3 du code de la sécurité intérieure et, d'autre part, de prévoir des garanties légales spécifiques faisant obstacle, par l'intermédiaire d'un accès administratif aux données de connexion, à la révélation d'une information à caractère secret dont un professionnel est le dépositaire, en particulier un avocat ou un journaliste ainsi que toute autre personne qui contribue directement à la collecte, la rédaction, la production ou la diffusion d'informations, par le biais d'un média, au profit du public.

POUR : **French Data Network (Réseau de données français), dite FDN**

La Quadrature du Net

Fédération des fournisseurs d'accès à Internet associatifs, dite Fédération FDN (FFDN)

SCP SPINOSI & SUREAU, avocat au conseil d'État

Question posée dans le cadre de la requête n° 388.134

Sur l'applicabilité au litige

I. La présente question prioritaire de constitutionnalité tend à faire constater la non-conformité à la Constitution des dispositions des articles L. 246-1, L. 246-2, L. 246-3, L. 246-4 et L. 246-5 du code de la sécurité intérieure, telles qu'issues de l'article 20 de la loi n° 2013-1168 du 18 décembre 2013 et insérées dans un Chapitre VI intitulé « *Accès administratif aux données de connexion* », en ce qu'elles disposent que :

Article 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 appelants, la durée et la date des communications. »

Article 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. »

Article 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. »

Article 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'Etat, 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 ».

II. Le litige à l'occasion duquel cette question a été soulevée procède du recours en annulation formé par les associations French Data Network (FDN) et La Quadrature du Net ainsi que par la Fédération des fournisseurs d'accès à Internet associatifs (FFDN) à l'encontre des dispositions du décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion.

Or, les dispositions de ce décret du 24 décembre 2014 ont bien été adoptées en application des dispositions contestées issues de l'article 20 de la loi n° 2013-1168 du 18 décembre 2013.

En effet, à l'exacte image de l'article 20 de cette loi n° 2013-1168 du 18 décembre 2013 qui insère un Chapitre VI intitulé « Accès administratif aux données de connexion » dans la partie législative du code de la sécurité intérieure, le décret du 24 décembre 2014 crée un chapitre également intitulé « Accès administratif aux données de connexion » au sein de la partie réglementaire du même du même code.

Certes, seules les dispositions de l'article L. 246-4 du code de la sécurité intérieure renvoient explicitement à un décret en Conseil d'Etat le soin de « *précise[r] notamment la procédure de suivi des*

demandes et les conditions et durée de conservation des informations ou documents transmis ».

Toutefois, le décret du 24 décembre 2014 n'a pas pour objet exclusif la mise en œuvre de ces seules dispositions de l'article L. 246-4 du code de la sécurité intérieure mais de l'ensemble des dispositions du Chapitre VI du titre IV du Livre II du code de la sécurité intérieure en sa partie législative.

Ainsi, l'article R. 241-1 de ce code, tel qu'issu du décret du 24 décembre 2014, prévoit que :

*« **Pour l'application de l'article L. 246-1**, les informations et les documents pouvant faire, à l'exclusion de tout autre, l'objet d'une demande de recueil sont ceux énumérés aux articles R. 1013 et R. 10-14 du code des postes et des communications électroniques et à l'article 1er du décret n° 2011219 du 25 février 2011 modifié relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne. »*

De même, l'article R. 241-2 du même code, tel qu'issu du décret du 24 décembre 2014, fixe « *les services relevant des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget dont les agents peuvent solliciter les informations et les documents mentionnés à l'article L. 246-1* » en indiquant explicitement que ces dispositions sont prises « **pour l'application du I de l'article L. 246-2** ».

En outre, l'alinéa 4 de l'article R. 246-7 du code de la sécurité intérieure précisent que :

*« **La sollicitation du réseau prévue à l'article L. 246-3** est effectuée par l'opérateur qui exploite le réseau. Les informations ou les documents demandés sont transmis, enregistrés, conservés et effacés dans les conditions prévues à l'article R. 246-6 ».*

III. Dans ces conditions, les dispositions des articles L. 246-1, L. 246-2, L. 246-3, L. 246-4 et L. 246-5 du code de la sécurité intérieure, telles qu'issues de l'article 20 de la loi n° 2013-1168 du

18 décembre 2013 sont bien applicables au litige né de la requête tendant à l'annulation de ces dispositions réglementaires – étant rappelé qu'une « *disposition est regardée comme applicable au litige si elle n'est pas étrangère au débat contentieux, qu'elle entretient un lien suffisant avec lui. Et le doute profite à l'auteur de la question* » (Alexandre Lallet et Xavier Domino, « An I ap. QPC », *AJDA*, 2011, p. 375).

Puisque les dispositions du décret ont été prises en application des dispositions législatives contestées, l'annulation de celles-ci par la présente question prioritaire de constitutionnalité privera nécessairement de tout fondement les dispositions réglementaires objet du recours en annulation devant le Conseil d'Etat.

La condition de l'applicabilité au litige est donc parfaitement et indiscutablement remplie quant à ces dispositions législatives.

Sur l'absence de déclaration de constitutionnalité antérieure

IV. Les dispositions des articles L. 246-1 à L. 246-5 du code de la sécurité intérieure ont été créées par l'article 20 de la 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.

Or, ces dispositions n'ont pas déjà été déclarées conformes à la Constitution dans les motifs et le dispositif d'une décision du Conseil constitutionnel.

D'une part, la loi n° 2013-1168 du 18 décembre 2013 n'a pas fait l'objet d'un contrôle de constitutionnalité *a priori* au titre de l'article 61 de la Constitution.

D'autre part, les articles L. 246-1 à L. 246-5 du code de la sécurité intérieure issus de cette même loi n'ont pas davantage été examinés par le Conseil constitutionnel dans le cadre d'une décision prise sur le fondement de l'article 61-1 de la Constitution.

La condition d'absence de déclaration préalable de conformité est donc, elle aussi, parfaitement remplie.

Sur le caractère nouveau

V. Il en va de même pour la condition tirée du caractère nouveau de la question.

V-1 En effet, la présente question prioritaire de constitutionnalité tend à faire constater que les dispositions des articles L. 246-1 à L. 246-5 du code de la sécurité intérieure portent notamment atteinte au droit au secret des échanges et correspondances entre un avocat et son client ou ses confrères et le droit au secret des sources d'information journalistiques entendues au sens large.

Ainsi qu'il le sera plus amplement détaillé, cette question tend à démontrer la méconnaissance par le législateur de sa compétence en ce que les dispositions litigieuses ont manqué de prévoir des garanties légales faisant obstacle à la révélation, par l'intermédiaire d'un accès administratif aux données de connexion, d'une information à caractère secret dont un professionnel est le dépositaire, en particulier un avocat ou un journaliste ainsi que toute autre personne qui contribue directement à la collecte, la rédaction, la production ou la diffusion d'informations, par le biais d'un média, au profit du public.

Ainsi, le législateur s'est abstenu d'assortir le dispositif d'accès administratif aux données de connexions prévu aux articles L. 246-1, à L. 246-5 du code de la sécurité intérieure de garanties appropriées et spécifiques aux fins de protéger **le droit au respect de la vie privée** ainsi que **la liberté d'expression et de communication**, dont découle le droit au secret des échanges et correspondances entre un avocat et son client ou ses confrères et le droit au secret des sources d'information journalistiques entendues au sens large.

V-2 Or, à ce jour, le Conseil constitutionnel n'a pas encore eu l'occasion d'affirmer explicitement l'existence de ce droit au secret des échanges et correspondances entre un avocat et son client ou ses confrères ainsi que de ce droit au secret des sources d'information journalistiques, ni même de préciser leur étendue.

V-2.1 Certes, au titre du droit au respect de la vie privée, l'importance du secret professionnel a d'ores et déjà été soulignée à plusieurs reprises par le Conseil constitutionnel (Cons. constit. Déc. n° 2009-581 DC du 25 juin 2009, cons. 7 et 8 ; Cons. constit. 2007-556 DC du 16 août 2007, cons. 31 ; Cons. constit. Dec. n° 2007-553 DC du 3 mars 2007, cons. 4 à 6).

De plus, d'une part, parmi les différents secrets professionnels ainsi protégés, **celui dont jouit l'avocat afin de garantir la confidentialité de ses échanges et correspondances avec ses clients ou ses confrères** revêt une intensité particulière.

En effet, un tel secret ne repose pas seulement sur le droit au respect de la vie privée ainsi protégé au titre de l'article 2 de la Déclaration des droits, mais aussi sur **les droits de la défense** ainsi que sur **le droit à procès équitable** chacun garanti par l'article 16 de la même Déclaration (v. respectivement Cons. Constit. Dec. n° 2006-535 DC du 30 mars 2006, cons. 24 ; 2011-214 QPC du 27 janvier 2012, cons. 5 et 6 ; et Cons. Constit. Dec. n° 2006-540 DC du 27 juillet 2006, cons. 11 ; 2012-247 QPC du 16 mai 2012, cons. 3, 5 à 7).

D'autre part, l'un des corollaires les plus essentiels de la liberté d'expression et de communication réside dans **le droit au secret des sources d'information journalistiques** entendues au sens large.

Puisque cette liberté d'expression et communication « *est une condition de la démocratie et l'une des garanties du respect des autres droits et libertés* » (Cons. Const., Déc. n° 2010-3 QPC, 28 mai 2010 et 2013-302 QPC, 12 avril 2013), elle a nécessairement pour vocation de garantir **le libre débat public** et **la libre diffusion de l'information**. Partant, c'est à l'aune du droit à l'information du public qu'il convient de garantir de protéger « *la libre communication des pensées et des opinions* ».

Or, dans ce contexte, si « *tout Citoyen peut donc parler, écrire, imprimer librement* » – selon les dispositions de l'article 11 de la Déclaration de 1789 –, il est manifeste qu'une telle liberté de communication est encore plus précieuse et cruciale pour **les journalistes**, lesquels ne peuvent exercer leur mission au service de

l'information du public et du débat public que si le secret de leurs sources est assuré par des garanties légales effectives.

Par extension, il en est également ainsi pour toute autre personne qui contribue directement à la collecte, la rédaction, la production ou la diffusion d'informations, par le biais d'un média, au profit du public, pour reprendre l'expression présente notamment au sein des dispositions de l'article 2 de la loi belge du 7 avril 2005 relative à la protection des sources journalistiques.

V-2.2 Certes, à ce stade, le Conseil constitutionnel n'a pas encore formellement et explicitement reconnu une valeur constitutionnelle au droit au secret des échanges et correspondances entre un avocat et son client ou ses confrères ainsi qu'au droit au secret des sources d'information journalistiques.

Tout au plus, s'agissant du premier droit, le Conseil a-t-il déjà eu l'occasion d'examiner la constitutionnalité de dispositions législatives garantissant le droit aux étrangers en rétention d'accéder « *en toutes circonstances, "sauf en cas de force majeure", à un espace pour s'entretenir confidentiellement avec leur avocat* », mais sans aucunement préciser la valeur d'un tel principe de confidentialité (Cons. Constit. Dec. n° 2003-484 DC du 20 novembre 2003, cons. 49 à 53).

En particulier, le Conseil constitutionnel n'a pas encore précisé de façon générale les conditions dans lesquelles le législateur doit encadrer les dispositifs d'accès à des données personnelles susceptibles de porter atteinte à de tels secrets.

Dans ces conditions, est nouvelle la question de savoir si le législateur peut, sans méconnaître le droit au secret des échanges et correspondances entre un avocat et son client ou ses confrères ainsi qu'au droit au secret des sources d'information journalistiques, s'abstenir d'assortir un tel dispositif des garanties légales appropriées et spécifiques.

Or, tel est précisément l'objet de la présente question prioritaire de constitutionnalité visant les dispositions des articles L. 246-1 à L. 246-5 du code de la sécurité intérieure.

V-3 Il résulte de ce qui précède que cette question sera l'occasion pour le Conseil constitutionnel de se prononcer sur l'existence, la portée et l'étendue du droit au secret des échanges et correspondances entre un avocat et son client ou ses confrères ainsi que du droit au secret des sources d'information journalistiques entendues au sens large.

De sorte qu'eu égard à son caractère nouveau, la présente question prioritaire de constitutionnalité ne pourra qu'être transmise au Conseil constitutionnel.

Sur le caractère sérieux

VI. Ce constat s'impose avec d'autant plus de force qu'au surplus, cette question présente **un caractère sérieux** en ce qu'en édictant les dispositions litigieuses portant création d'un dispositif d'« *accès administratif aux données de connexion* », le législateur a méconnu sa compétence en affectant ces droits et libertés que la Constitution garantit, notamment le droit au respect de la vie privée et la liberté de communication.

VII. Sur ce point, il y a lieu de rappeler d'emblée que le vice d'incompétence négative peut être utilement invoqué à l'occasion d'une question prioritaire de constitutionnalité dès lors qu'« *est affecté un droit ou une liberté que la Constitution garantit* » (Cons. constit., Déc. n° 2010-5 QPC du 18 juin 2010, *SNC KIMBERLY CLARK [Incompétence négative en matière fiscale]*).

Autrement dit, peut être invoqué au soutien d'une question prioritaire de constitutionnalité le moyen tiré d'une délégation de prérogatives du législateur au pouvoir réglementaire, dès lors que, d'une part, cette délégation est irrégulière au regard de la théorie de l'incompétence négative, et, d'autre part, la méconnaissance en cause de l'article 34 affecte des droits et libertés au sens de l'article 61-1, le législateur omettant d'encadrer, par des garanties de valeur législative, un tel droit ou une telle liberté.

En effet, cette omission est susceptible de priver de garanties légales des exigences constitutionnelles, ce que le juge constitutionnel ne saurait admettre.

Or, en l'occurrence, les exposantes entendent faire valoir qu'en édictant les dispositions litigieuses, c'est **à deux égards** que le législateur a méconnu sa propre compétence en affectant des droits et libertés que la Constitution garantit.

VIII. En premier lieu, le législateur a méconnu l'étendue de sa compétence **en s'abstenant totalement de définir**, d'une part, les notions d' « *informations ou documents* » prévues par les dispositions de l'article L. 246-1 du code de la sécurité intérieure et, d'autre part, la notion de « *sollicitation du réseau* » prévue par les dispositions de l'article L. 246-3 du même code.

Corrélativement, le législateur n'a pas davantage assorti ces notions de garanties légales suffisantes et appropriées afin d'éviter une extension excessive du champ d'application du dispositif d'accès administratif aux données de connexion.

Ainsi, le législateur a délégué indûment au pouvoir réglementaire le soin de déterminer le champ d'application d'un dispositif particulièrement attentatoire au droit au respect de la vie privée.

VIII-1 En effet, en droit, en vertu de l'article 34 mais aussi de « *l'objectif de valeur constitutionnelle d'intelligibilité et d'accessibilité de la loi, qui découle des articles 4, 5, 6 et 16 de la Déclaration des droits de l'homme et du citoyen de 1789* », le Conseil constitutionnel considère que, pour que le législateur puisse être regardé comme ayant pleinement exercé sa compétence, encore faut-il que celui-ci « **adopte des dispositions suffisamment précises et des formules non équivoques** » (Cons. Constit. Déc. n° 2006-540 DC, 27 juillet 2006, *Loi relative au droit d'auteur et aux droits voisins dans la société de l'information*, cons. 9).

Surtout, le juge constitutionnel a également précisé que :

« [Le législateur] doit en effet prémunir les sujets de droit contre une interprétation contraire à la Constitution ou contre le risque d'arbitraire, sans reporter sur des autorités administratives ou juridictionnelles le soin de fixer des règles dont la détermination n'a été confiée par la Constitution qu'à la loi » (Ibidem).

VIII-2 Or, et encore en droit, l'article 34 de la Constitution dispose notamment que :

« *La loi fixe les règles concernant :*

- les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ».

Autrement dit, la Constitution dispose que **seule la loi** peut définir les conditions dans lesquelles les citoyens peuvent jouir des libertés publiques. Il incombe donc au législateur d'assortir de garanties légales suffisantes les dispositions qui pourraient affecter lesdites libertés. Ce qui implique qu'il ne peut pas abandonner au pouvoir réglementaire la détermination du champ d'application des règles qu'il pose au sujet de l'exercice des libertés publiques.

VIII-3 Or, parmi ces libertés publiques figure indubitablement le droit au respect de la vie privée, garanti par l'article 2 de la Déclaration des droits de l'homme.

En effet, aux termes des dispositions de l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 :

« Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression ».

Sur ce fondement, le Conseil constitutionnel a estimé que « *la liberté proclamée par cet article implique le respect de la vie privée* » (Cons. Constit., Déc. n° 99-416 DC du 23 juillet 1999, cons. 45).

C'est au titre de cette « *liberté personnelle* » dont dérive le respect de la vie privée que le Conseil examine la constitutionnalité des

dispositifs législatifs relatifs à la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel (Cons. Constit., Déc. n° 2012-652 DC du 22 mars 2012, cons. 8).

VIII-4 De façon générale, le Conseil constitutionnel exerce un contrôle strict sur les conditions dans lesquelles le législateur autorise « *la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel* » (Cons. Constit., Déc. n° 2012-652 DC du 22 mars 2012, cons. 8).

En vertu du « *droit au respect de la vie privée et [d]es garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* », il est d'abord requis que les dispositions législatives relatives aux données personnelles « *comporte[nt] **les garanties appropriées et spécifiques** répondant aux exigences de l'article 34 de la Constitution* » (Cons. Constit., Déc. n° 2004-499 DC du 29 juillet 2004, cons. 11).

En d'autres termes, le Conseil veille à ce qu'en ce domaine, le législateur « *ne prive pas de **garanties légales des exigences constitutionnelles*** » (Cons. Constit., Déc. n° 2012-652 DC du 22 mars 2012, cons. 7 et 2004-499 DC du 29 juillet 2004, cons. 12).

Ensuite, et surtout, la juridiction constitutionnelle exige que « *la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel [soient] **justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif*** » (Cons. Constit. Déc. n° 2012-652 DC du 22 mars 2012, cons. 8).

A cet égard, et à l'instar de tout dispositif susceptible de porter atteinte à la liberté personnelle, il importe que « *le législateur [prenne] des mesures assurant, entre la protection de la santé et la protection de l'ordre public, d'une part, et la liberté personnelle, protégée par l'article 2 de la Déclaration de 1789, d'autre part, **une conciliation qui n[est] pas manifestement disproportionnée*** » (Cons. Constit., Déc. n° 2010-71 QPC du 26 novembre 2010, cons. 32).

En somme, sauf à méconnaître le droit constitutionnel au respect de la vie privée, le législateur ne peut y apporter une restriction que si celle-ci répond à de **solides conditions de justification ainsi que de proportionnalité** et si le législateur prévoit pour ce faire des **garanties légales appropriées et spécifiques**.

VIII-5 Ainsi, le Conseil constitutionnel a censuré pour incompétence négative affectant « *le droit au respect de la vie privée et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* » les dispositions de la loi du 29 juillet 2004 modifiant l'article 9 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Après avoir souligné « *qu'en raison de l'ampleur que pourraient revêtir les traitements de données personnelles ainsi mis en œuvre et de la nature des informations traitées, le 3° du nouvel article 9 de la loi du 6 janvier 1978 pourrait affecter, par ses conséquences, le droit au respect de la vie privée et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* » et « *que la disposition critiquée doit dès lors comporter les garanties appropriées et spécifiques répondant aux exigences de l'article 34 de la Constitution* », le Conseil a jugé que tel n'était pas le cas pour les dispositions alors contestées :

« S'agissant de l'objet et des conditions du mandat en cause, la disposition critiquée n'apporte pas ces précisions ; qu'elle est ambiguë quant aux infractions auxquelles s'applique le terme de « fraude » ; qu'elle laisse indéterminée la question de savoir dans quelle mesure les données traitées pourraient être partagées ou cédées, ou encore si pourraient y figurer des personnes sur lesquelles pèse la simple crainte qu'elles soient capables de commettre une infraction ; qu'elle ne dit rien sur les limites susceptibles d'être assignées à la conservation des mentions relatives aux condamnations ; qu'au regard de l'article 34 de la Constitution, toutes ces précisions ne sauraient être apportées par les seules autorisations délivrées par la Commission nationale de l'informatique et des libertés ; qu'en l'espèce et eu égard à la matière concernée, le législateur ne pouvait pas non plus se contenter, ainsi que le prévoit la disposition critiquée éclairée par les débats parlementaires, de poser une règle de principe

*et d'en renvoyer intégralement les modalités d'application à des lois futures ; que, par suite, le 3° du nouvel article 9 de la loi du 6 janvier 1978 est **entaché d'incompétence négative** » (Cons. constit., Dec. n° 2004-499 DC du 29 juillet 2004, cons. 11 et 12).*

IX. Or, en l'occurrence, et d'une part, le législateur s'est abstenu de définir les notions d'« *informations ou documents* » susceptibles d'être recueillis par les autorités administratives visées au I de l'article L. 246-2 du code de la sécurité intérieure.

IX-1 En effet, aux termes de ces dispositions de l'article L. 246-1 du code de la sécurité intérieure, sont évoquées 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. »

Il importe de souligner d'emblée que, **compte tenu de l'usage de l'expression « y compris »**, la liste des éléments ainsi susceptibles de figurer parmi ces « informations ou documents » n'est **aucunement limitative**.

Ainsi, ce sont donc la totalité des éléments « *traités ou conservés par leurs réseaux ou services de communications électroniques* », sans aucune exclusive, qui sont susceptibles de faire l'objet d'un recueil administratif.

En ce sens, dans son avis sur le projet de décret relatif à l'accès administratif aux données de connexion, la Commission nationale de l'informatique et des libertés (CNIL) a souligné que :

« L'article L. 246-1 du CSI dispose en effet que les demandes peuvent concerner des informations ou documents, y compris les données

limitativement prévues par le cadre juridique en vigueur. Cette formulation pourrait être interprétée comme permettant un élargissement des données pouvant être requises par rapport à celles pouvant actuellement être demandées aux opérateurs, qui sont limitées à des données d'identification » (CNIL, Délibération n° 2014-484 du 4 décembre 2014 portant avis sur un projet de décret relatif à l'accès administratif aux données de connexion et portant application de l'article L. 246-4 du code de la sécurité intérieure, JORF n° 0298 du 26 décembre 2014, texte n° 251).

Dans un communiqué du 20 décembre 2013, où elle déplorait n'avoir pas été saisie de l'examen de ces dispositions, la CNIL a été encore plus explicite en indiquant que :

*« Le recours à la notion **très vague** "d'informations et documents" traités ou conservés par les réseaux ou services de communications électroniques, semble permettre aux services de renseignement d'avoir accès **aux données de contenu**, et non pas seulement aux données de connexion (contrairement à ce qu'indique le titre du chapitre du Code de la sécurité intérieure créé par ces dispositions). Elle considère qu'une telle extension, réalisée dans le cadre du régime administratif du recueil des données de connexion, risque d'entraîner une atteinte disproportionnée au respect de la vie privée » (CNIL, « Promulgation de la loi de programmation militaire : la CNIL fait part de sa position », Communiqué du 20 décembre 2013).*

La doctrine n'a pas non plus manqué de mettre en exergue cette grave aporie législative.

Ainsi, le Professeur Laure Marino a indiqué que :

*« Malheureusement, la rédaction du texte **ne permet pas d'écarter sans hésitation l'accès au contenu**, en raison de son étrange formulation (l'« y compris » pose problème). Le seul titre du chapitre suffit-il à limiter le champ ? » (Laure Marino, « Surveillance du net : un Patriot Act à la française ? », in *Recueil Dalloz*, 2014, n° 5, p. 360).*

A propos de ces mêmes dispositions, d'autres observateurs soulignent également que :

*« La formulation retenue par le projet de loi de programmation militaire vise non seulement les données de connexion, mais **encore beaucoup plus largement** les informations et documents stockés par l'hébergeur »* (Claudine Guerrier, « Les interceptions et la loi de programmation militaire », in *Revue Lamy – Droit de l'immatériel*, 2014, n° 104, p. 95 ; en ce sens, lire aussi Willy Duhon, « L'imbroglie juridique de la conservation des données de connexion », in *Revue Lamy – Droit de l'immatériel*, 2014, n° 103, p. 86 : « La lecture ne laisse nul doute quant à l'interprétation : la rédaction de l'article [L. 246-1] considère que l'accès aux données porte sur des documents et des informations, au sens large, au titre desquelles une partie est constituée des données de connexion »).

IX-2 A cet égard, le contraste est particulièrement saisissant entre les dispositions litigieuses du code de la sécurité intérieure et celles de l'article L. 34-1-1 du code des postes et des communications électroniques, lesquelles régissaient le dispositif de recueil administratif des données de connexion jusqu'à leur abrogation au 1^{er} janvier 2015.

Initialement créées pour trois années par la loi n° 2006-64 du 23 janvier 2006, avant d'être prolongées jusqu'au 31 décembre 2015 par les lois n°s 2008-1245 du 1^{er} décembre 2008 et n° 2012-1432 du 21 décembre 2012, les dispositions de l'article L. 34-1-1, alinéa 1^{er}, du code des postes et des communications électroniques prévoyaient ainsi que :

« Afin de prévenir les actes de terrorisme, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions peuvent exiger des opérateurs et personnes mentionnés au I de l'article L. 34-1 la communication des données conservées et traitées par ces derniers en application dudit article ».

Surtout, aux termes de son deuxième alinéa, il était précisé que :

*« Les données pouvant faire l'objet de cette demande **sont limitées** aux 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, 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 appelants, la durée et la date des communications ».

Ainsi, le législateur avait bien pris soin de définir précisément et de manière limitative les différentes « données » susceptibles de faire l'objet d'un recueil administratif.

C'est d'ailleurs notamment à l'aune de cette précision législative que le Conseil constitutionnel avait déclaré partiellement conforme à la Constitution ces dispositions législatives.

En effet, saisi des dispositions du I de l'article 6 de la loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, lesquelles ont inséré dans le code des postes et des communications électroniques un nouvel article L. 34-1-1, le Conseil constitutionnel a d'abord rappelé que :

« Il appartient au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public, nécessaire à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des libertés constitutionnellement garanties, au nombre desquelles figurent le respect de la vie privée et la liberté d'entreprendre, respectivement protégés par les articles 2 et 4 de la Déclaration des droits de l'homme et du citoyen de 1789 » (Cons. constit., Déc. n° 2005-532 DC du 19 janvier 2006, cons. 9).

Or, à cet égard et en l'occurrence, le Conseil a jugé que :

« Le législateur a assorti la procédure de réquisition de données techniques qu'il a instituée de limitations et précautions, précisées ci-dessus, propres à assurer la conciliation qui lui incombe entre, d'une part, le respect de la vie privée des personnes et la liberté d'entreprendre des opérateurs, et, d'autre part, la prévention des actes terroristes, à laquelle concourt ladite procédure » (Ibid., cons. 10).

En particulier, il a été expressément relevé par le Conseil qu'aux termes des dispositions de l'article L. 34-1-1 du code des postes et des

communications électroniques, la procédure de réquisition administrative de données techniques de connexion :

« Sera **limitée** “aux 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, 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 appelants, maintien de la durée et la date de la communication“ » (Ibid., cons. 2).

IX-3 En s'abstenant d'assortir la définition de la notion « informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques » prévue à l'article L. 246-1 du code de la sécurité intérieure de telles « limitations et précautions » requises par le Conseil constitutionnel, le législateur a donc nécessairement autorisé « la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel » (Cons. constit., Déc. n° 2012-652 DC du 22 mars 2012, cons. 8) sans prévoir « les garanties appropriées et spécifiques répondant aux exigences de l'article 34 de la Constitution » (Cons. constit., Déc. n° 2004-499 DC du 29 juillet 2004, cons. 11).

Plus précisément encore, le législateur « priv[é] de garanties légales des exigences constitutionnelles » (Cons. constit., Déc. n° 2012-652 DC du 22 mars 2012, cons. 7 et 2004-499 DC du 29 juillet 2004, cons. 12), faute d'avoir précisé **explicitement** et **au sein même** des dispositions litigieuses la définition des données susceptibles de faire l'objet d'un tel recueil administratif.

IX-4 En particulier, si ces dispositions de l'article L. 246-1 du code de la sécurité intérieure désignent « *les opérateurs de communications électroniques et [l]es personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que [l]es 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* » comme possibles destinataires des

demandes d'accès administratif aux données de connexion, le législateur ne précise **aucunement** si les « *informations ou documents* » prévues par l'article L. 246-1 sont similaires aux données évoquées au sein de ces autres textes.

Au demeurant, ces autres définitions législatives sont fort peu homogènes.

Ainsi, selon les dispositions de l'article L. 34-1 du code des postes et des communications électroniques, sont successivement évoquées :

- « *Toute donnée relative au trafic* » (au point II) ;
- « *Certaines catégories de données techniques* » déterminées d'ailleurs par « *un décret en Conseil d'Etat* » (au point III) ;
- Des données portant « *sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux* » (au point IV).

Les dispositions de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ne sont pas davantage plus univoques et se distinguent d'ailleurs des définitions précédentes.

En effet, au point II de l'article précité sont évoquées « *les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires* ».

En somme, aucune définition unique et univoque ne procède ni dispositions contestées elles-mêmes, ni des autres dispositions législatives auxquelles les premières renvoient.

Le doute est d'autant plus permis que cette même expression d'« *informations et documents* » est déjà présente au sein du code de la sécurité intérieure, en son article L. 244-2, au sujet du régime d'interception judiciaire :

*« Les juridictions compétentes pour ordonner des interceptions en application du code de procédure pénale ainsi que le Premier ministre ou, en ce qui concerne l'exécution des mesures prévues à l'article L. 241-3, le ministre de la défense ou le ministre de l'intérieur peuvent recueillir, auprès des personnes physiques ou morales exploitant des réseaux de communications électroniques ou fournisseurs de services de communications électroniques, **les informations ou documents** qui leur sont nécessaires, chacun en ce qui le concerne, pour la réalisation et l'exploitation des interceptions autorisées par la loi.*

*La fourniture **des informations ou documents** visés à l'alinéa précédent ne constitue pas un détournement de leur finalité au sens de l'article 226-21 du code pénal. »*

Or, dans ce contexte précis, la notion d'« *informations ou documents* » renvoie à une interception bien plus vaste des contenus et non aux seules « *données de connexion* » (en ce sens, v. Willy Duhon, « L'imbroglia juridique de la conservation des données de connexion », in *Revue Lamy – Droit de l'immatériel*, 2014, n° 103, p. 86).

IX-5 Au surplus, les travaux préparatoires de la loi n° 2013-1168 du 18 décembre 2013 confirment indéniablement cette forte imprécision définitionnelle.

Car si de tels travaux préparatoires ne sauraient en aucune façon compenser une telle imprécision, ils peuvent néanmoins attester de ces carences législatives sources d'incompétence négative.

A cet égard, il importe de rappeler que l'article 20 de cette loi dont est issu le Chapitre VI du code de la sécurité intérieure intitulé « *Accès administratif aux données de connexion* » procède d'un amendement parlementaire initié le 20 octobre 2013 devant le Sénat en première lecture (N° 15 rect. ter).

Il n'a donc donné lieu à aucune étude d'impact et, au fil de la discussion parlementaire, aucune définition n'a été qu'esquissée.

Tout au plus est-il évoqué de manière récurrente, parmi ces « *données de connexion* », les « *fadettes* » mais **sans aucune exclusive** (v. ainsi Jean-Jacques HUEST, Discussion au Sénat en séance publique du 21 octobre 2013: « *toutes les autres données techniques, comme les fadettes, notamment, relèvent du contrôle a posteriori de la CNCIS* » ; v. aussi l'avis n° 1531 du député Patrice VERCHERE émis en première lecture à l'Assemblée Nationale au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, 6 novembre 2013 : « *Ce dispositif [d'accès administratif aux données de connexion] propose un dispositif unique de recueil administratif des données de connexion, qu'il s'agisse de données relatives aux communications passées (les factures détaillées ou « fadettes ») ou à la localisation des équipements permettant ces communications* »).

Manifestement, le libellé extrêmement imprécis des dispositions de l'article L. 246-1 du code de la sécurité intérieure est donc à l'image de l'incertitude qui a plané au cours des débats parlementaires.

IX-6 Dans ces conditions, la définition de la notion d'« *informations ou documents* » ainsi visée par les dispositions précitées n'a fait l'objet d'**aucune définition légale univoque**.

Ainsi, les dispositions litigieuses en viennent nécessairement à « *faire dépendre le champ d'application* » d'un dispositif d'accès administratif aux données de connexion, en soi particulièrement intrusif et attentatoire au droit au respect de la vie privée, de « *l'appréciation* » des autorités administratives elles-mêmes, ce qui « *méconnaît l'étendue de la compétence que le législateur tient de l'article 34 de la Constitution* » (v. *mutatis mutandis* Cons. constit., Déc. n° 98-399 DC du 5 mai 1998, cons. 7).

De ce seul fait, ces dispositions de l'article L. 246-1 du code de la sécurité intérieure sont **entachées d'une incompétence négative**.

X. D'autre part, le législateur a également manqué de définir la notion de « *sollicitation du réseau* » prévue par les dispositions de l'article L. 246-3 du code de la sécurité intérieure.

Plus précisément, le législateur n'a pas assorti cette notion de **garanties légales suffisantes et appropriées** afin d'éviter une extension excessive du champ d'application de ce dispositif d'accès administratif aux données de connexion, lequel est d'autant plus attentatoire au droit au respect de la vie privée qu'il intervient « *en temps réel* », ce qui est inédit.

X-1 En effet, aux termes des dispositions de l'alinéa 1^{er} de l'article L. 246-3 du code de la sécurité intérieure :

« 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 ».

Or, en raison de cette formulation, le législateur a manqué de préciser les conditions dans lesquelles les données de connexion pourraient ainsi être recueillies en temps réel et, en particulier, si une telle « *sollicitation du réseau* » pouvait donner lieu à un accès direct à ces données par les autorités administratives ou « *agents* » visés à l'article L. 246-2 du code de la sécurité intérieure.

De telles carences ont d'ailleurs été mises en exergue par la Commission nationale de l'informatique et des libertés (CNIL).

Dans son avis sur le projet de décret relatif à l'accès administratif aux données de connexion, la CNIL a ainsi souligné que :

« S'agissant des modalités concrètes de recueil de des données, la commission relève qu'une garantie est prévue par les dispositions réglementaires soumises pour avis, à savoir que « la sollicitation du réseau [...] est effectuée par l'opérateur qui exploite le réseau ». Il en résulte que cette formulation interdit toute possibilité d'aspiration massive et directe des données par les services concernés et, plus généralement, tout accès direct des agents des services de renseignement aux réseaux des opérateurs, dans la mesure où l'intervention sur les réseaux concernés est réalisée par les opérateurs de communication eux-mêmes » (CNIL, Délibération n° 2014-484 du 4 décembre 2014 portant avis sur un projet de décret relatif à l'accès administratif aux données de connexion et portant

application de l'article L. 246-4 du code de la sécurité intérieure, JORF n° 0298 du 26 décembre 2014, texte n° 251).

De fait, aux termes des dispositions de l'article R. 246-7, alinéa 4, du code de la sécurité intérieure, telles qu'issues du décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion :

« La sollicitation du réseau prévue à l'article L. 246-3 est effectuée par l'opérateur qui exploite le réseau. Les informations ou les documents demandés sont transmis, enregistrés, conservés et effacés dans les conditions prévues à l'article R. 246-6 ».

Or, si une telle précision par voie réglementaire fut nécessaire pour *« **interdi[re] toute possibilité d'aspiration massive et directe des données par les services concernés et, plus généralement, tout accès direct des agents des services de renseignement aux réseaux des opérateurs** »* (CNIL, précité), cela signifie nécessairement qu'une telle hypothèse n'était nullement exclue **par les dispositions législatives elles-mêmes**.

X-2 Une telle imprécision législative qui ouvre la voie à la possibilité d'un élargissement excessif par voie réglementaire des conditions de collecte des données de connexion a d'ailleurs été amplement dénoncée lors des débats parlementaires.

Ainsi, au soutien d'un amendement destiné à retirer la mention *« sur sollicitation du réseau »* aux motifs que cette *« expression [...] est floue, inopérante, et ne recouvre aucune réalité précise »* (Amendement n° 98 déposé le 23 novembre 2013 par les députés Tardy et de La Raudière), le député Lionel Tardy a indiqué que :

*« Il s'agit d'une demande de précision, car la notion de "sollicitation du réseau" me pose un problème : **elle est extrêmement floue**, reconnaissez-le, et ne veut pas dire grand-chose, si ce n'est rien du tout.*

Cet amendement vise à demander sa suppression, mais il s'agit d'un amendement d'appel pour inviter le Gouvernement et la commission à retravailler cette notion.

*Si j'ai bien compris, le but est l'interconnexion directe et en temps réel sur les réseaux des opérateurs. Or, je le répète, je ne comprends pas cette notion de "sollicitation du réseau". C'est pourtant mon métier. Soit elle va à l'encontre de l'objectif parce qu'elle est **trop large et sujette à interprétation**, soit elle est **tellement floue qu'elle donne carte blanche à une interconnexion sans filet**, ce qui serait intrusif. Dans les deux cas, ce n'est pas satisfaisant. J'aimerais savoir ce que recouvre cette notion. À mon sens, il faut que les opérateurs puissent intervenir, être consultés entre guillemets... Si c'est cela, autant le préciser car, en l'état, ce n'est pas clair du tout » (Compte rendu intégral des débats à l'Assemblée Nationale, Première séance du vendredi 29 novembre 2013).*

Nombre d'observateurs ont émis une analyse critique comparable en soulignant le flou qui enveloppe cette expression, en particulier en ce qu'elle permet un accès direct et permanent des agents désignés à l'article L. 246-2 du code de la sécurité intérieure :

*« L'accès est prévu en « temps réel », par « sollicitation du réseau », ce qui correspond à **un accès direct et permanent aux serveurs de l'hébergeur**. Il s'agit donc bien d'une forme de « perquisition » et se trouvent particulièrement menacés les documents stockés dans un service de Cloud souscrit par un internaute. » (Claudine Guerrier, « Les interceptions et la loi de programmation militaire », in *Revue Lamy – Droit de l'immatériel*, 2014, n° 104, p. 95).*

X-3 Partant, et là encore, la définition de la notion de « *sollicitation du réseau* » prévue à l'article L. 246-3 du code de la sécurité intérieure n'a fait l'objet d'**aucune définition légale univoque** et n'est pas davantage assortie de **garanties légales** susceptibles d'interdire au pouvoir réglementaire d'étendre les conditions d'accès aux données de connexion, au surplus dans le cadre d'un dispositif particulièrement intrusif puisque permettant une transmission « *en temps réel* ».

De ce chef, ces dispositions de l'article L. 246-3 du code de la sécurité intérieure sont elles-aussi **entachées d'incompétence négative**.

XI. A deux égards, donc, le législateur a indubitablement méconnu sa propre compétence, puisque les dispositions de l'article 34 lui confient le soin de fixer les règles concernant « *les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* ».

XII. Or, il ne fait aucun doute que cette méconnaissance de l'article 34 affecte des droits et libertés au sens de l'article 61-1 de la Constitution.

XII-1 En effet, le droit au respect de la vie privée figure parmi les « *droits et libertés* » au sens de cet article 61-1 de la Constitution (voir Cons. Constit., Dec. n° 2010-25 QPC du 16 septembre 2010, cons. 6 et 16).

A nouveau, il convient ainsi de rappeler que le Conseil constitutionnel a censuré pour incompétence négative affectant « *le droit au respect de la vie privée et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* » les dispositions de la loi du 29 juillet 2004 modifiant la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Et ce, au motif qu'elles ne « *comport[ai]ent pas les garanties appropriées et spécifiques répondant aux exigences de l'article 34 de la Constitution* », notamment parce que le législateur est demeuré « *ambiguë* » et a « *laissée indéterminée* » nombre de questions relatives aux traitements de données, ou encore « *n'a rien dit sur les limites susceptibles d'être assignées à la conservation des mentions relatives aux condamnations* » et s'est « content[é] de poser une règle de principe et d'en renvoyer intégralement les modalités d'application à des lois futures » (Cons. constit. Dec. n° 2004-499 DC du 29 juillet 2004, cons. 12).

XII-2 Or, en s'abstenant de définir d'une part, les notions d'« *informations ou documents* » prévues par les dispositions de l'article L. 246-1 du code de la sécurité intérieure et, d'autre part, la notion de « *sollicitation du réseau* » prévue par les dispositions de

l'article L. 246-3 du même code, le législateur a abandonné au pouvoir règlementaire la détermination de notions clefs susceptibles de faire varier significativement le champ d'application du dispositif d'accès aux données de connexion prévu par le Chapitre VI du Titre IV du Livre II du même code.

Par voie de conséquence, le législateur a renoncé à encadrer les conditions dans lesquelles des restrictions peuvent être apportées au droit au respect de la vie privée.

Dès lors, les dispositions législatives affectent indéniablement ce droit constitutionnellement garanti au titre de l'article 2 de la Déclaration de 1789.

XIII. Il résulte de tout ce qui précède que le législateur s'est non seulement abstenu de définir des notions d'« *informations ou documents* » et de « *sollicitation du réseau* » prévues respectivement par les dispositions des articles L. 246-1 et 246-3 du code de la sécurité intérieure mais, corrélativement, a également manqué d'assortir de garanties légales suffisantes ces dispositions relatives à un dispositif attentatoire au droit au respect de la vie privée.

Ces matières relevant à ne pas en douter du domaine législatif, le législateur a, de ce chef déjà, **méconnu l'étendue de sa compétence en affectant des droits et libertés que la Constitution garantit.**

Mais il y a plus.

XIV. En second lieu, et de surcroît, la méconnaissance par le législateur de sa compétence est d'autant plus patente que les dispositions litigieuses ont également manqué de prévoir des garanties légales faisant obstacle à la révélation, par l'intermédiaire d'un accès administratif aux données de connexion, d'une information à caractère secret dont un professionnel est le dépositaire, en particulier un avocat ou un journaliste, ainsi que toute autre personne qui contribue directement à la collecte, la rédaction, la production ou la diffusion d'informations, par le biais d'un média, au profit du public.

Ainsi, le législateur s'est abstenu d'assortir le dispositif d'accès administratif aux données de connexions prévu aux articles L. 246-1 à L. 246-5 du code de la sécurité intérieure de garanties appropriées et spécifiques aux fins de protéger **le droit au respect de la vie privée** ainsi que **la liberté d'expression et de communication**, dont découle notamment le droit au secret des échanges et correspondances entre un avocat et son client ou ses confrères et le droit au secret des sources d'information journalistiques entendues au sens large.

XIV-1 En effet, en droit, au nom de l'article 34, le Conseil constitutionnel a précisé que le législateur doit :

« Prémunir les sujets de droit contre une interprétation contraire à la Constitution ou contre le risque d'arbitraire, sans reporter sur des autorités administratives ou juridictionnelles le soin de fixer des règles dont la détermination n'a été confiée par la Constitution qu'à la loi » (Cons. Constit. Déc. n° 2006-540 DC, 27 juillet 2006, *Loi relative au droit d'auteur et aux droits voisins dans la société de l'information*, cons. 9).

XIV-2 Or, et encore en droit, l'article 34 de la Constitution dispose notamment que :

« La loi fixe les règles concernant :

- les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; la liberté, le pluralisme et l'indépendance des médias ».

Autrement dit, la Constitution dispose que **seule la loi** peut définir les conditions dans lesquelles les citoyens peuvent jouir des libertés publiques.

De plus, les principes de liberté, de pluralisme et d'indépendance des médias ne peuvent également être protégés que **par des dispositions légales**.

Il incombe donc au législateur d'assortir de garanties légales suffisantes les dispositions qui pourraient affecter lesdites libertés. Ce

qui implique qu'il ne peut pas abandonner au pouvoir réglementaire ni la détermination du champ d'application des règles qu'il pose au sujet de l'exercice des libertés publiques, ni la fixation de garanties susceptible de protéger ces dernières.

Parmi ces libertés publiques figure indubitablement le droit au respect de la vie privée, garanti par l'article 2 de la Déclaration des droits de l'homme, ainsi que **le droit constitutionnel au secret des sources d'information journalistiques** qui découle de la liberté de communication.

XIV-3 En effet, et **d'une part**, il importe de rappeler qu'aux termes des dispositions de l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 :

« Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression ».

XIV-3.1 Sur ce fondement, le Conseil constitutionnel a estimé que *« la liberté proclamée par cet article implique le respect de la vie privée »* (Cons. Constit., Déc. n° 99-416 DC du 23 juillet 1999, cons. 45).

C'est au titre de cette *« liberté personnelle »* dont dérive le respect de la vie privée que le Conseil examine la constitutionnalité des dispositifs législatifs relatifs à la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel (Cons. Constit., Déc. n° 2012-652 DC du 22 mars 2012, cons. 8).

A cet égard, et de nouveau, il convient de souligner que le Conseil constitutionnel exerce un contrôle strict sur les conditions dans lesquelles le législateur autorise *« la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel »* (Cons. Constit., Déc. n° 2012-652 DC du 22 mars 2012, cons. 8).

En vertu du « *droit au respect de la vie privée et [d]es garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* », il est d'abord requis que les dispositions législatives relatives aux données personnelles « *comporte[nt] les garanties appropriées et spécifiques répondant aux exigences de l'article 34 de la Constitution* » (Cons. Constit., Déc. n° 2004-499 DC du 29 juillet 2004, cons. 11).

En d'autres termes, le Conseil veille à ce qu'en ce domaine, le législateur « *ne prive pas de garanties légales des exigences constitutionnelles* » (Cons. Constit., Déc. n°s 2012-652 DC du 22 mars 2012, cons. 7 et 2004-499 DC du 29 juillet 2004, cons. 12).

Ensuite, et surtout, la juridiction constitutionnelle exige que « *la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel [soient] justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif* » (Cons. Constit., Déc. n° 2012-652 DC du 22 mars 2012, cons. 8).

En somme, sauf à méconnaître le droit constitutionnel au respect de la vie privée, le législateur ne peut y apporter une restriction que si celle-ci répond à de **solides conditions de justification ainsi que de proportionnalité** et si le législateur prévoit pour ce faire des **garanties légales appropriées et spécifiques** (en ce sens et dans le contexte des données personnelles, v. not. Cons. Constit., Dec. n° 2004-499 DC du 29 juillet 2004, cons. 11 et 12).

XIV-3.2 Dans ce cadre, le Conseil constitutionnel attache une importance particulière **au secret professionnel** qui bénéficie d'une protection au titre du droit au respect de la vie privée.

Ainsi, et notamment, si le Conseil a jugé conforme à la Constitution les dispositions du règlement relatif à l'organisation et au fonctionnement de l'Assemblée nationale relatives aux pouvoirs de convocation et d'audition des commissions permanentes, c'est après avoir dûment souligné que :

« La législation assurant la préservation du secret professionnel et du secret de la défense nationale interdit à toute personne qui en est dépositaire de révéler de tels secrets, même à l'occasion de son audition par une commission permanente » (Cons. Constit., Déc. n° 2009-581 DC du 25 juin 2009, cons. 7 et 8).

Dans le même sens, les dispositions de l'article 5 de la loi n° 2007-1224 du 21 août 2007 relatives aux déclarations individuelles de salariés ayant l'intention de participer à une grève n'ont pas été regardées comme contraire à la Constitution, dès lors que ces déclarations :

« Sont couvertes par le secret professionnel ; que leur utilisation à d'autres fins ou leur communication à toute personne autre que celles désignées par l'employeur comme étant chargées de l'organisation du service sera passible des peines prévues à l'article 226-13 du code pénal ; que, dans le silence de la loi déferée, les dispositions de la loi du 6 janvier 1978 susvisée s'appliquent de plein droit aux traitements de données à caractère personnel qui pourraient éventuellement être mis en oeuvre ; qu'ainsi, l'obligation de déclaration individuelle s'accompagne de garanties propres à assurer, pour les salariés, le respect de leur droit à la vie privée » (Cons. constit., 2007-556 DC du 16 août 2007, cons. 31).

Enfin, si le Conseil constitutionnel peut admettre que, dans certaines hypothèses, des personnes soient déliées de leur secret professionnel, c'est à la condition que le législateur l'ait dûment « prévu » et ce, aux termes d'une stricte « conciliation entre, d'une part, l'exercice des libertés constitutionnellement garanties, au nombre desquelles figure le droit au respect de la vie privée et, d'autre part, les exigences de solidarité découlant des dixième et onzième alinéas du Préambule de 1946 » (Cons. constit. Dec. n° 2007-553 DC du 3 mars 2007, cons. 4 à 6).

XIV-3.3 Parmi les différents secrets professionnels ainsi protégés au titre du droit au respect de la vie privée, **celui dont jouit l'avocat afin de garantir la confidentialité de ses échanges et correspondances avec ses clients ou ses confrères** revêt une intensité particulière.

En effet, il convient de souligner qu'un tel secret ne repose pas seulement sur le droit au respect de la vie privée ainsi protégé au titre de l'article 2 de la Déclaration des droits, mais aussi sur **les droits de la défense** ainsi que sur **le droit à procès équitable** chacun garanti par l'article 16 de la même Déclaration (v. respectivement Cons. Constit., Dec. n^{os} 2006-535 DC du 30 mars 2006, cons. 24 ; 2011-214 QPC du 27 janvier 2012, cons. 5 et 6 ; et Cons. Constit. Dec. n^{os} 2006-540 DC du 27 juillet 2006, cons. 11 ; 2012-247 QPC du 16 mai 2012, cons. 3, 5 à 7).

Certes, à ce stade, le Conseil constitutionnel n'a pas encore formellement et explicitement reconnu une valeur constitutionnelle au droit au secret des échanges et correspondances entre un avocat et son client ou ses confrères.

Tout au plus a-t-il déjà eu l'occasion d'examiner la constitutionnalité de dispositions législatives garantissant le droit aux étrangers en rétention d'accéder « *en toutes circonstances, "sauf en cas de force majeure", à un espace pour s'entretenir confidentiellement avec leur avocat* », mais sans aucunement préciser la valeur d'un tel principe de confidentialité (Cons. Constit., Dec. n^o 2003-484 DC du 20 novembre 2003, cons. 49 à 53).

Néanmoins, à l'instar du droit à « *l'assistance effective d'un avocat* » (Cons. Constit., Déc. n^{os} 2010-14/22 QPC du 30 juillet 2010, cons. 28 ; 2011-191/194/195/196/197 QPC du 18 novembre 2011, cons. 19 et 20) ou du « *principe du caractère contradictoire de la procédure* » (Cons. Constit., Déc. n^{os} 84-184 DC du 29 décembre 1984, cons. 36; 89-268 DC du 29 décembre 1989, cons. 58), il ne fait guère de doute qu'un tel droit au secret constitue **un corollaire du principe des droits de la défense ainsi que du droit à un procès équitable**.

Tel est d'ailleurs le sens univoque de la jurisprudence de la Cour de cassation, laquelle garantit avec constance **le « *principe de la confidentialité des conversations téléphoniques entre un avocat et un client* »** (v. not. Cass. crim., 18 janvier 2006, n^o 05-86.447).

Et ce, en visant tout particulièrement l'article 66-5 de la loi n^o 71-1130 du 31 décembre 1971 – aux termes duquel les correspondances et autres pièces échangées entre un avocat et son client ou ses

confrères « *sont couvertes par le secret professionnel* » – ainsi que l'article 100-5 du code de procédure pénale dont les dispositions prévoient que :

« *A peine de nullité, ne peuvent être transcrites les correspondances avec un avocat relevant de l'exercice des droits de la défense* ».

De plus, la Cour de cassation vise également l'article 8 de la Convention européenne des droits de l'homme.

De fait, c'est sur ce fondement que la Cour européenne des droits de l'homme – dont la jurisprudence est examinée avec attention par le Conseil constitutionnel – souligne avec force et constance l'importance cruciale de la protection accordée à la confidentialité des échanges entre avocats et clients.

Ainsi, dans un récent arrêt *Michaud c. France*, la Cour a encore rappelé que :

« ***En vertu de l'article 8, la correspondance entre un avocat et son client, quelle qu'en soit la finalité (la correspondance strictement professionnelle étant incluse : Niemietz précité, § 32), jouit d'un statut privilégié quant à sa confidentialité (Campbell c. Royaume-Uni, 25 mars 1992, §§ 46-48, série A no 233 ; voir aussi, notamment, Ekinci et Akalin c. Turquie, no 77097/01, 30 janvier 2007, § 47 ; cela vaut, comme indiqué précédemment, pour toutes les formes d'échanges entre les avocats et leurs clients). Elle a en outre indiqué qu'elle « accorde un poids singulier au risque d'atteinte au secret professionnel des avocats car il peut avoir des répercussions sur la bonne administration de la justice* » (Wieser et Bicos précité, §§ 65-66 ; voir aussi, précités, Niemietz, § 37, et André, § 41) et est la base de la relation de confiance entre l'avocat et son client (André, précité, § 41, et Xavier da Silveira, précité, § 36).** » (Cour EDH, Anc. 5^e Sect., 6 décembre 2012, *Michaud c. France*, Req. n° 12323/11, § 117)

Cette forte protection imposée par la Cour européenne est notamment justifiée par des impératifs liés au droit de la défense et, plus largement, au procès équitable :

« Il en résulte que si l'article 8 protège la confidentialité de toute « correspondance » entre individus, **il accorde une protection renforcée aux échanges entre les avocats et leurs clients**. Cela se justifie par le fait que les avocats se voient confier une mission fondamentale dans une société démocratique : **la défense des justiciables**. Or un avocat ne peut mener à bien cette mission fondamentale s'il n'est pas à même de garantir à ceux dont il assure la défense que leurs échanges demeureront confidentiels. C'est la relation de confiance entre eux, **indispensable à l'accomplissement de cette mission**, qui est en jeu. En dépend en outre, indirectement mais nécessairement, **le respect du droit du justiciable à un procès équitable, notamment en ce qu'il comprend le droit de tout « accusé » de ne pas contribuer à sa propre incrimination**.

Cette **protection renforcée** que l'article 8 confère à la confidentialité des échanges entre les avocats et leurs clients et les raisons qui la fondent, conduisent la Cour à constater que, pris sous cet angle, le secret professionnel des avocats – qui toutefois se décline avant tout en obligations à leur charge – est **spécifiquement protégé par cette disposition** » (Michaud c. France, précité, § 118 et 199).

En outre, et dans le même sens, une non moins récente directive de l'Union européenne 2013/48/UE du 22 octobre 2013 a prévu en son article 4 que :

« Les États membres respectent la confidentialité des communications entre les suspects ou les personnes poursuivies et leur avocat dans l'exercice du droit d'accès à un avocat prévu par la présente directive. Ces communications comprennent les rencontres, la correspondance, les conversations téléphoniques et **toute autre forme de communication autorisée par le droit national** ».

Il y a d'ailleurs lieu de noter que de telles exigences européennes s'appliquent pleinement dans le contexte des données personnelles, la Cour de justice de l'Union européenne ayant récemment invalidé la directive 2006/24 relative à la conservation de ces données aux motifs, notamment, que celle-ci :

« Ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel » (CJUE, Grande Chambre,

8 avril 2014, *Digital Rights Ireland et Seitlinger e.a.*, Aff. C-293/12 et C-594/12, § 58).

Or, les fortes garanties ainsi reconnues au principe de confidentialité au plan européen ne sauraient être moindres sur le plan constitutionnel, alors que l'ensemble des droits et libertés ainsi dédiés au respect de la vie privée, au procès équitable et aux droits de la défense sont parfaitement convergents.

Dans ces conditions, il ne fait aucun doute que le droit au secret des échanges et correspondances entre un avocat et son client ou ses confrères relève lui-aussi des droits et libertés que la Constitution garantit au sens de l'article 61-1, au même titre que du droit au respect de la vie privée, du principe des droits de la défense ainsi que du droit à un procès équitable dont il découle.

XIV-4 D'autre part, la liberté de communication des pensées et des opinions est garantie par les dispositions de l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789, lesquels prévoient que :

« La libre communication des pensées et des opinions est un des droits les plus précieux de l'Homme : tout Citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la Loi ».

Or, très tôt, le Conseil constitutionnel a affirmé que :

*« La communication des idées et des informations [...] intéresse [...] une des libertés publiques dont les garanties fondamentales relèvent de la disposition précitée de l'article 34 » (Cons. Constit., Déc. n° 64-27 L, 17 et 19 mars 1964, *Nature juridique de certaines dispositions des articles 1^{er}, 5, 6, 7 bis et 11 de l'ordonnance n° 59-273 du 4 février 1959 relative à la Radiodiffusion-Télévision française, ainsi que de celles de l'article 70 de la loi n° 61-1396 du 21 décembre 1961 portant loi de finances pour 1962*, cons. 2 ; voir également, pour un exemple récent, Cons. Constit., Déc. n° 2012-647 DC, 28 février 2012, *Loi visant à réprimer la contestation de l'existence des génocides reconnus par la loi*, cons. 5).*

XIV-5 En ce sens, il y a d'ailleurs lieu de relever que le Conseil constitutionnel retient une conception extensive de la compétence du législateur en matière de liberté de communication.

Cette liberté est en effet regardée comme « *une condition de la démocratie et l'une des garanties du respect des autres droits et libertés* » (Cons. Constit., Déc. n^{os} 2010-3 QPC du 28 mai 2010, cons. 6).

Le Conseil constitutionnel a ainsi jugé que « *le législateur a méconnu l'étendue de sa compétence* » en « *renvo[yant] à un décret en Conseil d'État le soin de préciser [l]es conditions d'application* » d'un dispositif fixant « *les principes d'attribution des noms de domaine* » Internet, au motif notamment qu'une telle délégation affectait la liberté de communication garantie à l'article 11 de la Déclaration de 1789 (Cons. Constit., Déc. n^o 2010-45 QPC, 6 octobre 2010, *M. Mathieu P.*, cons. 5 et 6).

En ce domaine, le Conseil exige donc du législateur qu'il ne « *rest[e pas] en deçà de la compétence que lui confie l'article 34 de la Constitution pour fixer" les règles concernant... les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques"* » (Cons. Constit., Dec. n^o 2007-550 DC du 27 février 2007, cons. 17) et qu'il assortisse les dispositions ayant trait à la liberté de communication de « *garantie[s] fondamentale[s] pour l'exercice d'une liberté publique* », lesquelles « *relève[nt] de la compétence exclusive du législateur* » (Cons. Constit. Dec. n^o 84-173 DC du 26 juillet 1984, cons. 3).

XIV-6 Or, et ainsi qu'il a été dit, puisque la liberté de communication « *est une condition de la démocratie* et l'une des garanties du respect des autres droits et libertés » (Cons. Constit., Déc. n^{os} 2010-3 QPC, 28 mai 2010 et 2013-302 QPC, 12 avril 2013), une telle liberté constitutionnelle a nécessairement pour vocation de garantir **le libre débat public** et **la libre diffusion de l'information**.

XIV-6.1 En effet, selon une jurisprudence constante du Conseil constitutionnel, les citoyens sont, dans leur ensemble, « *au nombre*

des destinataires essentiels de la liberté [d'expression et de communication] proclamée par l'article 11 de la Déclaration de 1789 » (voir, pour les lecteurs de la presse écrite, Cons. Constit., Déc. n° 86-210 DC, 29 juillet 1986, *Loi portant réforme du régime juridique de la presse*, cons. 20, pour les auditeurs et téléspectateurs, Cons. Constit., Déc. n° 93-333 DC, 21 janvier 1994, *Loi modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication*, cons. 3).

Partant, c'est à l'aune du droit à l'information du public qu'il convient de garantir de protéger « *la libre communication des pensées et des opinions* ».

Or, dans ce contexte, si « *tout Citoyen peut donc parler, écrire, imprimer librement* » – selon les dispositions de l'article 11 de la Déclaration de 1789 –, il est manifeste qu'une telle liberté de communication est encore plus précieuse et cruciale pour **les journalistes** ainsi que, plus largement, pour toute autre personne qui contribue directement à la collecte, la rédaction, la production ou la diffusion d'informations, par le biais d'un média, au profit du public.

En effet, la nature et l'essence même de leur mission impliquent qu'ils soient directement au service de l'information du public et du débat public.

A ce titre, les journalistes – et plus largement encore, toute autre personne qui contribue directement à la collecte, la rédaction, la production ou la diffusion d'informations, par le biais d'un média, au profit du public – doivent jouir d'une indépendance ainsi que d'une liberté accrue.

XIV-6.2 Or, l'un des corollaires les plus essentiels de la liberté d'expression journalistique, entendue en ce sens large, réside dans **le droit au secret des sources d'information**.

Définie classiquement, notamment par la Déclaration des devoirs et des droits des journalistes du 24 novembre 1971, dite « *Déclaration de Munich* », comme le droit des journalistes « *de garder le secret professionnel et ne pas divulguer la source des informations obtenues*

confidentiellement », ce droit au secret des sources d'informations bénéficie d'une forte reconnaissance au plan international, européen et national.

A cet égard et tout particulièrement, la liberté constitutionnelle de communication peut là encore être utilement éclairée par la jurisprudence de la Cour européenne des droits de l'homme relative à la liberté conventionnelle d'expression.

Ce parallèle est d'autant plus justifié en matière de liberté de communication qu'ainsi que le relèvent des commentateurs avisés de la doctrine constitutionnaliste, « *le Conseil constitutionnel se place dans la droite ligne de la jurisprudence européenne en matière de liberté d'expression* » (Wanda Mastor et Jean-Gabriel Sorbara, « Réflexions sur le rôle du Parlement à la lumière de la décision du Conseil constitutionnel sur la contestation des génocides reconnus par la loi », in *RFDA*, 2012, n° 3, p. 510).

Ainsi, selon une jurisprudence aussi solennelle que constante, la Cour européenne affirme que :

« La protection des sources journalistiques est l'une des pierres angulaires de la liberté de la presse, comme cela ressort des lois et codes déontologiques en vigueur dans nombre d'Etats contractants et comme l'affirment en outre plusieurs instruments internationaux sur les libertés journalistiques (voir notamment la Résolution sur les libertés journalistiques et les droits de l'homme, adoptée à la 4e Conférence ministérielle européenne sur la politique des communications de masse (Prague, 7-8 décembre 1994), et la Résolution du Parlement européen sur la non-divulgence des sources journalistiques du 18 janvier 1994, parue au Journal officiel des Communautés européennes no C 44/34).

L'absence d'une telle protection pourrait dissuader les sources journalistiques d'aider la presse à informer le public sur des questions d'intérêt général. En conséquence, la presse pourrait être moins à même de jouer son rôle indispensable de "chien de garde" et son aptitude à fournir des informations précises et fiables pourrait s'en trouver amoindrie.

*Eu égard à l'importance que revêt la protection des sources journalistiques pour la liberté de la presse dans une société démocratique et à l'effet négatif sur l'exercice de cette liberté que risque de produire une ordonnance de divulgation, pareille mesure ne saurait se concilier avec l'article 10 (art. 10) de la Convention que si elle se justifie par un impératif prépondérant d'intérêt public » (Cour EDH, G.C. 27 mars 1996, *Goodwin c. Royaume-Uni*, Req. n° 17488/90, § 39).*

L'importance ainsi reconnue à la protection des sources n'a cessé d'être réaffirmée, la Cour de Strasbourg ayant notamment souligné que :

*« Le droit des journalistes de taire leurs sources ne saurait être considéré comme un simple privilège qui leur serait accordé ou retiré en fonction de la licéité ou de l'illicéité des sources, mais **un véritable attribut du droit à l'information**, à traiter avec la plus grande circonspection » (Cour EDH, 4^e Sect., 25 février 2003, *Tillack c. Belgique*, n° 20477/05, § 65).*

Plus récemment encore, la Grande Chambre de la Cour européenne a encore renforcé ces principes protecteurs en jugeant que :

*« Compte tenu de l'importance vitale pour la liberté de la presse de la protection des sources des journalistes et des informations susceptibles de conduire à leur identification, toute atteinte au droit à la protection de pareilles sources doit être entourée de **garanties procédurales, définies par la loi, en rapport avec l'importance du principe en jeu** » (Cour EDH, G.C. 14 septembre 2010, *Sanoma Uitgevers B.V. c. Pays-Bas*, Req. n° 38224/03, § 88)*

Or, il a été souligné que :

*« Au premier rang des garanties exigées doit figurer la possibilité de faire **contrôler la mesure par un juge ou tout autre organe décisionnel indépendant et impartial**. Le principe selon lequel, dans les affaires concernant la protection des sources des journalistes, « le tribunal doit pouvoir contempler le tableau complet de la situation » a été souligné dans l'une des toutes premières affaires de cette nature examinées par les organes de la Convention (*British Broadcasting Corporation*, précitée (paragraphe 54 ci-dessus)). Le contrôle requis*

*doit être mené par un organe, **distinct de l'exécutif et des autres parties intéressées, investi du pouvoir de dire, avant la remise des éléments réclamés, s'il existe un impératif d'intérêt public l'emportant sur le principe de protection des sources des journalistes** et, dans le cas contraire, d'empêcher tout accès non indispensable aux informations susceptibles de conduire à la divulgation de l'identité des sources.* » (Ibid. § 90).

Même en cas d'urgence, la Cour exige qu'« un **contrôle indépendant** [soit] mené à tout le moins avant que les éléments obtenus ne soient consultés et exploités devrait être suffisant pour permettre de déterminer si une question de confidentialité se pose et, le cas échéant, si, eu égard aux circonstances particulières de l'espèce, l'intérêt public invoqué par les autorités d'enquête ou de poursuite l'emporte sur l'intérêt public général à la protection des sources » (Ibid. § 91).

A nouveau, il convient également de rappeler que le droit de l'Union européenne offre lui aussi une forte protection au secret professionnel, la Cour de justice de l'Union européenne ayant récemment invalidé la directive 2006/24 relative à la conservation des données personnelles aux motifs, notamment, que celle-ci :

« *Ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, **au secret professionnel*** » (CJUE, Grande Chambre, 8 avril 2014, *Digital Rights Ireland et Seitlinger e.a.*, Aff. C-293/12 et C-594/12, § 58).

Ainsi, à l'exacte image du droit au secret des échanges et correspondances entre un avocat et son client ou ses confrères, il ne saurait être question de conférer au **droit au secret des sources d'information journalistiques** une protection constitutionnelle moindre que celle qui lui est fermement reconnu au plan européen.

Au surplus, un tel droit au secret des sources d'information est le corollaire de deux importants droits et libertés que la Constitution garantit, en l'occurrence la liberté de communication mais aussi le droit au respect de la vie privée.

Dans ces conditions, ce droit au secret des sources d'information relève lui aussi et indéniablement des droits et libertés que la Constitution garantit au sens de l'article 61-1.

XV. Certes, une telle reconnaissance constitutionnelle ne signifie aucunement que le droit au secret des échanges et correspondances entre un avocat et son client ou ses confrères, d'une part, et le droit au secret des sources d'information, d'autre part, bénéficient d'une protection absolue.

A l'instar de l'ensemble des droits et libertés que la Constitution garantit, chacun de ces droits peut faire l'objet de restrictions notamment au nom d'autres impératifs et droits constitutionnels.

Toutefois, de telles restrictions doivent être « *justifié[s] par un motif d'intérêt général et mis[es] en œuvre de manière adéquate et proportionnée à cet objectif* » (v. *mutatis mutandis* Cons. constit., Déc. n° 2012-652 DC du 22 mars 2012, cons. 8).

Surtout, le législateur ne saurait « *prive[r] de garanties légales d[e] telles exigences constitutionnelles* » (v. Cons. Constit., Déc. n° 2012-652 DC du 22 mars 2012, cons. 7 ; 2004-499 DC du 29 juillet 2004, cons. 12) et doit s'assurer que ces dispositions « *comporte[nt] les garanties appropriées et spécifiques répondant aux exigences de l'article 34 de la Constitution* » (Cons. constit. Déc. n° 2004-499 DC du 29 juillet 2004, cons. 11).

Or, en l'occurrence, tel n'est absolument pas le cas des dispositions litigieuses.

XVI. En effet, les dispositions des articles L. 246-1 à L. 246-5 du code de la sécurité intérieure, telles qu'issues de l'article 20 de la loi n° 2013-1168 du 18 décembre 2013, prévoient un dispositif d'accès administratif aux données de connexion. Et ce, en ne prévoyant aucune garantie légale susceptible de faire efficacement obstacle à la révélation, par l'intermédiaire d'un tel accès administratif, d'une information à caractère secret dont un professionnel est le dépositaire, en particulier un avocat ou un journaliste ainsi que toute autre personne qui contribue directement à la collecte, la rédaction, la

production ou la diffusion d'informations, par le biais d'un média, au profit du public.

XVI-1 Certes, nul ne peut contester qu'au-delà du seul code de la sécurité intérieure, d'autres dispositions législatives offrent une protection contre la révélation de telles informations relevant du secret professionnel.

Ainsi, et d'une part, aux termes des dispositions de l'article 226-13 du code pénal, il est prévu que :

« La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende ».

D'autre part, outre cette incrimination générale destinée à prohiber en principe toute atteinte au secret professionnel, d'autres dispositions offrent des garanties particulières au profit de certaines professions.

Il en est ainsi, d'abord, **des avocats**.

Aux termes des dispositions de l'article 66-5, alinéa 1^{er}, de la loi n° 71-1130 du 31 décembre 1971 :

*« En toutes matières, que ce soit dans le domaine du conseil ou dans celui de la défense, les consultations adressées par un avocat à son client ou destinées à celui-ci, les correspondances échangées entre le client et son avocat, entre l'avocat et ses confrères à l'exception pour ces dernières de celles portant la mention " officielle ", les notes d'entretien et, plus généralement, toutes les pièces du dossier **sont couvertes par le secret professionnel** ».*

De plus, selon les dispositions de l'article 100-5, alinéa 3, du code de procédure pénale :

« A peine de nullité, ne peuvent être transcrites les correspondances avec un avocat relevant de l'exercice des droits de la défense ».

Il en est de même, ensuite, s'agissant des journalistes.

Selon les dispositions de l'article 2 de la loi du 29 juillet 1881 sur la liberté de la presse, telles qu'issues de la loi n° 2010-1 du 4 janvier 2010 relative à la protection du secret des sources des journalistes :

« Le secret des sources des journalistes est protégé dans l'exercice de leur mission d'information du public.

Est considérée comme journaliste au sens du premier alinéa toute personne qui, exerçant sa profession dans une ou plusieurs entreprises de presse, de communication au public en ligne, de communication audiovisuelle ou une ou plusieurs agences de presse, y pratique, à titre régulier et rétribué, le recueil d'informations et leur diffusion au public.

*Il ne peut être porté atteinte directement ou indirectement au secret des sources **que** si un impératif prépondérant d'intérêt public le justifie et si les mesures envisagées sont strictement nécessaires et proportionnées au but légitime poursuivi. Cette atteinte ne peut en aucun cas consister en une obligation pour le journaliste de révéler ses sources.*

*Est considéré comme une atteinte indirecte au secret des sources au sens du troisième alinéa le fait de **chercher à découvrir les sources d'un journaliste** au moyen d'investigations portant sur toute personne qui, en raison de ses relations habituelles avec un journaliste, peut détenir des renseignements permettant d'identifier ces sources.*

Au cours d'une procédure pénale, il est tenu compte, pour apprécier la nécessité de l'atteinte, de la gravité du crime ou du délit, de l'importance de l'information recherchée pour la répression ou la prévention de cette infraction et du fait que les mesures d'investigation envisagées sont indispensables à la manifestation de la vérité ».

Ces différentes interdictions ne sont toutefois assorties d'aucune sanction pénale.

Tout au plus la loi n° 2010-1 du 4 janvier 2010 a-t-elle inséré diverses garanties procédurales tenant notamment aux conditions de perquisition d'une entreprise de presse ou du domicile d'un journaliste

(article 56-2 du code de procédure pénale), à l'obligation pour un journaliste de témoigner devant une juridiction pénale (articles 326, alinéa 2, et 437, alinéa 2, du code de procédure pénale) ou à la transcription de correspondances avec un journaliste permettant d'identifier une source (article 100-5, alinéa 4, du code de procédure pénale).

XVI-2 Toutefois, compte tenu des insignes particularités du dispositif d'accès administratif aux données de connexion, l'ensemble de ces différentes garanties destinées à garantir le droit au secret professionnel sont parfaitement inapplicables et ineffectives dans un tel cadre.

XVI-2.1 En effet, et **premièrement**, ces garanties légales ont essentiellement pour vocation d'offrir une protection de ces secrets professionnels ainsi que de leurs dépositaires dans le cadre d'une procédure pénale.

Il en est ainsi des conditions de transcription des correspondances avec un avocat ou un journaliste (article 100-5, alinéas 3 et 4, du code de procédure pénale) ou de l'obligation de témoigner devant une juridiction pénale (articles 326, alinéa 2, et 437, alinéa 2, du code de procédure pénale).

Or, et ainsi que le Conseil constitutionnel l'a lui-même souligné lorsqu'il a été saisi des dispositions de l'article L. 34-1-1 du code des postes et des communications électroniques – lesquelles prévoyaient un dispositif comparable à celui issu des dispositions contestées de l'article 20 de la loi n° 2013-1168 – :

« Les réquisitions de données permises par les nouvelles dispositions constituent des mesures de police purement administrative ; qu'elles ne sont pas placées sous la direction ou la surveillance de l'autorité judiciaire, mais relèvent de la seule responsabilité du pouvoir exécutif ; qu'elles ne peuvent donc avoir d'autre finalité que de préserver l'ordre public et de prévenir les infractions ».

En d'autres termes, les dispositions du code de procédure pénale sont parfaitement inapplicables au dispositif d'accès administratif aux

données de connexion et ne peuvent donc être regardées comme des garanties légales des exigences constitutionnelles protégeant le secret professionnel, en particulier celui des avocats et des journalistes ainsi que toute autre personne qui contribue directement à la collecte, la rédaction, la production ou la diffusion d'informations, par le biais d'un média, au profit du public.

Pourtant, ce sont bien ces dispositions du code de procédure pénale qui offrent à ce droit au secret professionnel – et spécifiquement au droit au secret des échanges et correspondances entre un avocat et son client ou ses confrères, d'une part, et au **droit au secret des sources d'information** des journalistes, d'autre part – les garanties les plus effectives, si ce n'est les seules.

En effet, les autres dispositions générales, telles celles de l'article 66-5, alinéa 1^{er}, de la loi n° 71-1130 du 31 décembre 1971 et celles de l'article 2 de la loi du 29 juillet 1881 sur la liberté de la presse, se bornent à prévoir une interdiction d'atteinte au secret professionnel des avocats et journalistes sans l'assortir d'une quelconque sanction pénale ou garantie procédurale.

XVI-2.2 Deuxièmement, compte tenu des modalités particulières du dispositif d'accès administratif aux données de connexion, l'ensemble des dispositions légales protégeant le secret professionnel ne peuvent être mobilisées pour faire obstacle et réprimer d'éventuelles atteintes à ce secret du fait de ce dispositif.

En effet, aux termes des dispositions de l'article L. 246-1 du code de la sécurité intérieure, il convient de rappeler que ce sont les agents administratifs désignés à l'article L. 246-2 du même code qui ont vocation à recueillir :

« Des informations et documents [...] 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 ».

En vertu de l'article L. 246-3, alinéa 1^{er}, du code de la sécurité intérieure, ces mêmes informations et 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* ».

Dans ces conditions, ce sont soit les opérateurs désignés à l'article L. 246-1 du code de la sécurité intérieure, soit potentiellement et directement – en vertu de la notion de « *sollicitation du réseau* » (cf. *supra X et s.*) – les agents administratifs désignés à l'article L. 246-2 du même code, qui ont vocation à méconnaître le secret professionnel sans que les dépositaires initiaux du secret ne puissent s'y opposer.

Ainsi, à supposer même qu'il soit possible de réduire les « *informations et documents* » visés à l'article L. 246-1 du code de la sécurité intérieure aux seules données techniques de connexion des personnes, il est manifeste que celles-ci peuvent recéler des informations permettant de porter directement atteinte à la confidentialité des échanges entre un avocat et son client ou un de ses confrères – notamment en révélant l'existence, la fréquence, la durée et même la localisation des échanges téléphoniques et numériques entre ces derniers.

Ceci est encore plus manifeste concernant l'atteinte au secret des sources d'information journalistiques, comme en atteste avec éloquence la notoire affaire dite des « *fadettes du Monde* ».

Ainsi, pour confirmer l'annulation en appel des réquisitions ayant permis que soient menées des investigations sur les lignes téléphoniques de journalistes du journal *Le Monde*, la Cour de cassation a relevé qu'une telle pratique constitue effectivement :

« [Une] atteinte portée au secret des sources des journalistes [laquelle] n'était pas justifiée par l'existence d'un impératif prépondérant d'intérêt public et que la mesure n'était pas strictement nécessaire et proportionnée au but légitime poursuivi, [de sorte que] la chambre de l'instruction a légalement justifié sa décision, tant au regard de l'article 10 de la Convention européenne des droits de l'homme qu'au regard de l'article 2 de la loi du 29 juillet 1881 » (Cass. Crim., 6 décembre 2011, n° 11-83.970)

Or, dans ce contexte particulier, l'article 66-5, alinéa 1^{er}, de la loi n° 71-1130 du 31 décembre 1971 et l'article 2 de la loi du 29 juillet 1881 sur la liberté de la presse, lesquelles se bornent à consacrer respectivement le droit au secret professionnel des avocats et des journalistes sans l'assortir d'aucun mécanisme préventif ou répressif de nature à empêcher efficacement toute atteinte à ce droit.

A cet égard, l'incrimination prévue à l'article 226-13 du code pénal, laquelle réprime de façon générale « la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire », ne saurait être regardée comme suffisante.

Outre qu'en tout état de cause, une telle incrimination n'est pas de nature à **empêcher** que soit commise une violation du secret professionnel, laquelle est en soi susceptible d'emporter des conséquences irrémédiables, il n'est aucunement acquis qu'elle puisse davantage permettre **la répression effective** d'une telle violation.

En effet, compte tenu du principe d'interprétation stricte de la loi pénale et du principe constitutionnel de légalité des délits et des peines, le libellé de l'article 226-13 du code pénal semble difficilement permettre les poursuites et sanctions contre des opérateurs au seul motif que ceux-ci auraient, en déférant à une réquisition administrative, livré des « *informations et documents* » susceptibles de violer le secret professionnel, alors même qu'ils ne sont absolument pas en mesure de déterminer que ces éléments peuvent emporter la révélation d'un tel secret.

Plus sûrement encore, l'incrimination prévue à l'article 226-13 du code pénal ne permet aucune poursuite et sanction pénales contre les agents ayant sollicité ces informations, puisque ce dernier texte réprime seulement « la révélation d'une information à caractère secret **par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire** ». Or, les agents administratifs désignés à l'article L. 246-2 du code de la sécurité intérieure ne sont pas les auteurs de la révélation mais les bénéficiaires de celle-ci.

Dans ces conditions, il est manifeste que l'ensemble des garanties légales dédiées à la protection du secret professionnel, en particulier ceux des avocats et journalistes, sont radicalement contournées.

XVI-2.3 Une telle absence de garanties légales spécifiques contraste d'ailleurs singulièrement avec les dispositions de l'article 6, III-2, de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, par lesquelles le législateur a souhaité prévoir explicitement que :

« Les personnes mentionnées au 2 du I sont assujetties au secret professionnel dans les conditions prévues aux articles 226-13 et 226-14 du code pénal, pour tout ce qui concerne la divulgation de ces éléments d'identification personnelle ou de toute information ».

Il s'agissait ainsi de prévoir spécifiquement que « *les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services* », au sens de l'article 6, I-2, de la loi du 21 juin 2004, doivent respecter le secret professionnel.

Or, non seulement ces dispositions ne s'appliquent qu'à une partie seulement des opérateurs et personnes visés par l'article L. 246-1 du code de la sécurité intérieure, celui-ci désignant aussi les personnes mentionnées au I-1 de l'article 6 de la loi du 21 juin 2004 ainsi qu'à l'article L. 34-1 du code des postes et télécommunication.

Surtout, ce dispositif de l'article 6, III-2, de la loi du 21 juin 2004 ne prohibe que la révélation spontanée par l'opérateur de « *signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services* », et non la transmission sur réquisition administrative de données de connexion.

Or, une fois encore, il convient de rappeler qu'à supposer même que les opérateurs et personnes visés par l'article L. 246-1 du code de la sécurité intérieure puissent invoquer le secret professionnel pour s'opposer à une réquisition – ce que ne permettent pas les dispositions contestées –, il leur est en tout état de cause impossible de déterminer

parmi les différents « *documents et informations* » ceux qui pourraient relever du secret professionnel.

A tous égards, donc, les dispositions contestées ne prévoient aucune garantie protégeant **spécifiquement, explicitement et efficacement** le secret professionnel, en particulier celui des avocats et journalistes ainsi que de toute autre personne qui contribue directement à la collecte, la rédaction, la production ou la diffusion d'informations, par le biais d'un média, au profit du public.

XVI-3 Au demeurant, de telles carences manifestes ne sauraient être compensées par les seuls dispositifs de contrôle prévus par les dispositions contestées.

XVI-3.1 En effet, et d'abord, les demandes d'accès « *sur sollicitation du réseau et transmis en temps réel* » au sens de l'article L. 246-3 du code de la sécurité intérieure sont accordées « *par décision écrite du Premier ministre ou des personnes spécialement désignées par lui, pour une durée maximale de trente jours* ».

Dans ces conditions, la protection du secret professionnel, en particulier du droit au secret des sources d'informations journalistiques, n'est aucunement garanti puisque ce n'est pas « *un juge ou tout autre organe décisionnel indépendant et impartial* » qui exerce un contrôle « *avant la remise des éléments réclamés* », mais un organe qui n'est pas « *distinct de l'exécutif et des autres parties intéressées* » (en ce sens, v. not. Cour EDH, G.C. 14 septembre 2010, *Sanoma Uitgevers B.V. c. Pays-Bas*, Req. n° 38224/03, § 88).

XVI-3.2 Ensuite, s'agissant des demandes d'accès prévues par les dispositions de l'article L. 246-3, II du code de la sécurité intérieure, celles-ci sont « *soumises à la décision d'une personnalité qualifiée placée auprès du Premier ministre* ».

Or, si « *cette personnalité est désignée pour une durée de trois ans renouvelable par la Commission nationale de contrôle des interceptions de sécurité* », c'est « *sur proposition du Premier ministre* qui lui présente une liste d'au moins trois noms ».

Ce seul fait suffit à révéler que cette autorité de contrôle ne présente pas les garanties requises d'indépendance et d'impartialité, étant souligné que le législateur n'a prévu aucune autre garantie en ce sens.

XVI-3.3 De plus, la seule reconnaissance, par les dispositions de l'article L. 246-4 du code de la sécurité intérieure, « *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* » au profit de la Commission nationale de contrôle des interceptions de sécurité, ne saurait davantage constituer une garantie suffisante.

Outre que la Commission nationale de contrôle des interceptions de sécurité ne dispose d'aucun pouvoir de contrôle avant l'accès aux « *informations et documents* » afin d'empêcher une atteinte irrémédiable au secret professionnel, elle ne peut que formuler de simples recommandations – sans aucun pouvoir d'injonction – auprès du Premier ministre.

XVI-3.4 Enfin, et en tout état de cause, ni la « *personnalité qualifiée placée auprès du Premier ministre* » désignée à l'article L. 246-3, II du code de la sécurité intérieure, ni la Commission nationale de contrôle des interceptions de sécurité ne sont expressément et légalement habilitées par les dispositions contestées à déterminer si l'accès administratif aux données de connexion est susceptible de porter atteinte aux secrets professionnels, et en particulier à ceux des journalistes (en ce sens, v. *Sanoma Uitgevers B.V. c. Pays-Bas*, précité, § 96).

XVII. Partant, les dispositions des articles L. 246-1 à L. 246-5 du code de la sécurité intérieure qui prévoient un accès administratif aux données de connexion ont totalement manqué d'assortir ce dispositif des **garanties légales** indispensables à la protection du secret professionnel, en particulier du secret des échanges et correspondances entre un avocat et son client ou ses confrères et du

secret des sources d'information journalistiques entendues au sens large.

De ce chef, les dispositions précitées sont elles-aussi **entachées d'une incompétence négative** en ce que le législateur a manqué de fixer les règles concernant « *les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* » et « *la liberté, le pluralisme et l'indépendance des médias* » comme l'exige l'article 34 de la Constitution.

XVIII. Or, il ne fait aucun doute qu'une telle méconnaissance de l'article 34 affecte des droits et libertés au sens de l'article 61-1 de la Constitution.

XVIII-1 En effet, il convient de rappeler que tant le droit au respect de la vie privée que la liberté d'expression et de communication figurent parmi les « *droits et libertés* » au sens de cet article 61-1 de la Constitution (voir respectivement Cons. Constit., Dec. n° 2010-25 QPC du 16 septembre 2010, cons. 6 et 16 et Cons. Const., Déc. n° 2010-3 QPC du 28 mai 2010, cons. 6).

Au surplus, en tant que corollaire de ces droits et libertés, le droit au secret des échanges et correspondances entre un avocat et son client ou ses confrères et le droit au secret des sources d'information journalistiques entendues au sens large ne peuvent également manquer d'être également reconnus comme de tels droits au sens de l'article 61-1 de la Constitution.

En ces domaines, le Conseil constitutionnel exige donc du législateur qu'il ne « rest[e pas] en deçà de la compétence que lui confie l'article 34 de la Constitution pour fixer" les règles concernant... les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques" » (Cons. Constit., Dec. n° 2007-550 DC du 27 février 2007, cons. 17).

Plus précisément, les dispositions relatives à ces droits et libertés doivent « comporter les garanties appropriées et spécifiques répondant aux exigences de l'article 34 de la Constitution » (Cons. constit., Déc. n° 2004-499 DC du 29 juillet 2004, cons. 11), lesquelles

« relève[nt] de la compétence exclusive du législateur » (Cons. Constit., Dec. n° 84-173 DC du 26 juillet 1984, cons. 3).

XVIII-2 Or, en l'occurrence, le législateur a manqué de prévoir des garanties légales faisant obstacle à la révélation, par l'intermédiaire d'un accès administratif aux données de connexion, d'une information à caractère secret par une personne qui en est dépositaire, en particulier les avocats et les journalistes, ainsi que de toute autre personne qui contribue directement à la collecte, la rédaction, la production ou la diffusion d'informations, par le biais d'un média, au profit du public.

Ce faisant, le législateur s'est abstenu d'assortir le dispositif d'accès administratif aux données de connexions prévu aux articles L. 246-1, à L. 246-5 du code de la sécurité intérieure de garanties appropriées et spécifiques aux fins de protéger **le droit au respect de la vie privée** ainsi que **la liberté d'expression et de communication**, dont découle notamment le droit au secret des échanges et correspondances entre un avocat et son client ou ses confrères et le droit au secret des sources d'information journalistiques entendues au sens large.

Dès lors, les dispositions législatives affectent indéniablement ces droits constitutionnellement garantis au titre des articles 2, 11 et 16 de la Déclaration de 1789.

XIX. Il résulte de tout ce qui précède que de ce chef aussi, le législateur a **méconnu l'étendue de sa compétence en affectant des droits et libertés que la Constitution garantit.**

XX. Il résulte de l'ensemble des considérations précédemment énoncées que cette question prioritaire de constitutionnalité présente indéniablement un caractère sérieux.

De sorte qu'elle ne pourra qu'être transmise au Conseil constitutionnel.

PAR CES MOTIFS, et tous autres à produire, déduire, suppléer, au besoin même d'office, les exposantes concluent à ce qu'il plaise au Conseil d'Etat :

- **CONSTATER** l'existence du moyen contestant la conformité d'une disposition législative, aux droits et libertés garantis par la Constitution ;
- **TRANSMETTRE** au Conseil constitutionnel la question suivante :

« En édictant les dispositions des articles L. 246-1, L. 246-2, L. 246-3, L. 246-4 et L. 246-5 du code de la sécurité intérieure, le législateur a-t-il méconnu sa propre compétence en affectant des droits et libertés que la Constitution garantit, notamment le droit au respect de la vie privée et la liberté de communication, en ce qu'il s'est abstenu, d'une part, de définir les notions d' « informations ou documents » et de « sollicitation du réseau » prévues respectivement par les dispositions des articles L. 246-1 et L. 246-3 du code de la sécurité intérieure et, d'autre part, de prévoir des garanties légales spécifiques faisant obstacle, par l'intermédiaire d'un accès administratif aux données de connexion, à la révélation d'une information à caractère secret dont un professionnel est le dépositaire, en particulier un avocat ou un journaliste, ainsi que toute autre personne qui contribue directement à la collecte, la rédaction, la production ou la diffusion d'informations, par le biais d'un média, au profit du public ? »

Avec toutes conséquences de droit.

SPINOSI & SUREAU
SCP d'Avocat au Conseil d'État