SAISINE DU CONSEIL CONSTITUTIONNEL

Loi relative au renseignement

Monsieur le Président,
Mesdames et Messieurs les Conseillers,

Les signataires de la présente saisine auprès de votre Conseil, sur la loi sur le renseignement, partagent naturellement l'objectif principal de ce texte qui est de donner un cadre légal aux pratiques des services de renseignement, dans l'espoir qu'il permette de renforcer la sécurité des Français face aux nouvelles menaces terroristes.

Ce texte pose cependant la question très difficile de l'équilibre qu'il convient de trouver entre d'une part, le renforcement des moyens et la protection de nos services de renseignement, et d'autre part, la proportionnalité de leurs intrusions dans les libertés individuelles, et notamment la vie privée de chacun de nos concitoyens.

Nous nous interrogeons notamment, comme cela est développé dans les pages suivantes, sur la définition large et peu précise des missions pouvant donner lieu à enquêtes administratives ; sur les moyens techniques considérables de collectes massives de données ; ainsi que sur la proportionnalité, par rapport aux objectifs recherchés, de la mise en œuvre de ces techniques intrusives et attentatoires au respect de la vie privée, à l'ère où le numérique est présent à chaque instant de notre vie. La concentration des pouvoirs aux seules mains de l'Exécutif est d'autant plus préoccuppante, qu'à aucun moment il n'existe un véritable droit de recours du citoyen auprès du juge judicaire, garant des libertés individuelles selon notre Constitution.

Au moment où les Etats-Unis viennent de voter le « Freedom Act » en juin 2015 et font ainsi marche arrière par rapport au « Patriot Act », adopté suite aux attentats du 11 septembre 2001, il est étonnant de voir le gouvernement français présenter un projet de loi sur le renseignement, rédigé dans l'urgence, à la suite des attentats de janvier 2015 et examiné en procédure accélérée. L'étude d'impact du projet de loi est d'ailleurs peu documentée, voire pas du tout en ce qui concerne l'article 2 sur les algorithmes et les boites noires.

La discussion législative a montré que ces inquiétudes se sont manifestées dans tous les groupes politiques, sans esprit partisan. Il n'y a pas d'un côté ceux qui seraient déterminés à défendre la République et de l'autre, le camp des naïfs ou des mauvais patriotes, complaisants vis-à-vis du terrorisme. Notre démarche est tout simplement celle d'élus de la Nation, déterminés à la fois à se battre contre les terroristes et contre d'éventuelles dérives qui pourraient menacer nos libertés.

C'est dans ce contexte que nous vous communiquons cette saisine cosignée par XX députés.

*
* *

1°) SUR L'ARTICLE 1

A) En ce qui concerne l'article L. 811-3 du code de la sécurité intérieure

L'article 1er introduit au code de la sécurité intérieure un nouvel article L. 811-3 qui définit de manière limitative – encore que ce caractère limitatif aurait gagné à être exprimé par la disposition en cause qui, à la différence de l'ex-article L. 241-1 du code de la sécurité intérieure, ne mentionne plus que les interceptions de correspondances peuvent être autorisées « *à titre exceptionnel* » – les finalités permettant de recourir aux techniques de renseignement prévues par ailleurs par la loi.
Dans la mesure où ces techniques, qu'il n'est pas nécessaire de décrire pour l'instant, portent une atteinte forte à la vie privée et présentent aussi la caractéristique de recueillir des informations sur des personnes étrangères à la cible des services de renseignement (ex : IMSI-catcher), leur mise en œuvre doit être justifiée par des motifs non seulement légitimes mais encore énoncés en termes suffisamment précis.

Ainsi qu'on le sait, « *il appartient au législateur, en vertu de l'article 34 de la Constitution, de fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ;* […] *il lui appartient notamment d'assurer la conciliation entre, d'une part, la sauvegarde de l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la protection de principes et de droits de valeur constitutionnelle et, d'autre part, le respect de la vie privée et des autres droits et libertés constitutionnellement protégés* » (Cons. const., décision n° 2003-467 DC, 13 mars 2003, cons. 20).

En outre, il ressort de la jurisprudence constitutionnelle que la liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 implique le droit au respect de la vie privée, de sorte que « *la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif* » (Cons. const., décision n° 2012-652 DC, 22 mars 2012, cons. 8).

En vertu du « *droit au respect de la vie privée et des garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* », il est d'abord requis que les dispositions législatives relatives aux données personnelles « *comportent les garanties appropriées et spécifiques répondant aux exigences de l'article 34 de la Constitution* » (Cons. const., décision n° 2004-499 DC, 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. const., décision nos 2012-652 DC, 22 mars 2012, cons. 7 et 2004-499 DC, 29 juillet 2004, cons. 12).

Or, en l'occurrence, l'atteinte portée au droit au respect de la vie privée est dépourvue des garanties adéquates, à raison même de la sémantique législative utilisée qui conduit à autoriser le recours à ces techniques sans que cela résulte d'une nécessité publique avérée et dans des conditions si imprécises que toute garantie devient, par là-même, illusoire.

a) Il en va ainsi de l'énumération qui figure à l'article L. 811-3 du code de la sécurité

intérieure, lequel mentionne, non les intérêts « essentiels » de la politique étrangère de la France, ou encore les intérêts économiques, industriels et scientifiques de la France, mais les intérêts « *majeurs* » en ces domaines (2° et 3°).

Or, quels sont-ils ? La disposition attaquée est, sur ce point, si vague, qu'elle porte en elle un risque certain d'évasement dans le recours aux techniques de renseignement, alors que seule la nécessité publique peut justifier qu'elles soient mises en œuvre.
La notion d' « intérêts majeurs de la politique étrangère » ou les « intérêts économiques, industriels et scientifiques majeurs » n'est défini par aucune disposition constitutionnelle ou légale, de sorte que son contenu ressort alors de l'article 20 de la constitution disposant que « le Gouvernement détermine et conduit la politique de la Nation ». C'est donc le gouvernement qui détermine seul des intérêts essentiels de la politique étrangère, celle-ci étant subordonnée à la politique de la Nation. C'est aussi le gouvernement qui va déterminer – seul – les intérêts économiques, industriels et scientifiques majeurs ».

Ainsi, en autorisant le recours aux techniques de renseignement pour la poursuite de ces finalités, le législateur a laissé le gouvernement déterminer arbitrairement les critères lui permettant de porter atteinte aux droits et libertés fondamentaux des citoyens, sans que le présente loi ne le limite d'aucune façon, échouant à « prémunir les sujets de droit […] contre le risque d'arbitraire », tel que l'exige pourtant le Conseil constitutionnel dans sa décision n°2006-540 DC du 27 juillet 2006 (et de façon constante cf :2007-5557 DC du 15/11/2007 ; 2008-564DC du 19/6/2008 ; 2008-567 du 24/7/2008 ; 2013-685 du 29/12/2013).

Cette sémantique, trop relâchée, conduit ainsi à ce qu'il soit porté atteinte de manière disproportionnée au droit au respect de la vie privée.

b) Il en va de même du recours à ces techniques en ce qui concerne « *l'exécution des engagements européens et internationaux de la France* » (2°).

Cette finalité est énoncée en termes tellement lâches que les techniques de renseignement pourront à loisir être mises en œuvre par les services au prétexte commode que ces engagements sont en cause.

De même, que recouvre l'expression « *la prévention de toute forme d'ingérence étrangère* » (2°) ? Cette formule encourt des critiques identiques.

c) C'est, *mutatis mutandis*, également le cas des « *atteintes à la forme républicaine des institutions* » ou encore des « *violences collectives de nature à porter gravement atteinte à la paix publique* » (5°). Ces notions sont extrêmement vagues.

La « *forme républicaine* » (du gouvernement), si elle est mentionnée à l'article 89 de la Constitution, signifie, étymologiquement, le contraire de la monarchie, et on voit mal quelle autre réalité juridique elle pourrait recouvrir. Tout adhérent ou sympathisant à un parti politique se réclamant de la monarchie entrerait dans le champ d'application de cette loi et pourrait être l'objet des techniques de renseignement. Or, c'est l'article 4 de la constitution qui seul restreint l'activité des partis politiques en ce sens qu' « ils doivent respecter les principes de la souveraineté nationale et de la démocratie ».
Il conviendrait, *a minima*, que le conseil constitutionnel précise que cette notion s'entend au sens du chapitre 2 du livre IV du code pénal intitulé « Des autres atteintes aux institutions de la République ou à l'intégrité du territoire national » (art. 412-1 à 412-8).

De même, les « *violences collectives* » dont s'agit incluent, potentiellement, toute manifestation, dont il est au surplus difficile de déterminer à l'avance si elles porteront « *gravement atteinte à la paix publique* ». Le renseignement s'étend en réalité à toute manifestation, la notion d'atteinte à la paix publique étant purement préventive et comportant, de ce fait, une part de subjectivité substantielle.

À cet égard, il importe de rappeler qu'aux termes de la décision n° 94-352 DC, la liberté de manifester relève du « *droit d'expression collective des idées et des opinions ; qu'il appartient au législateur d'assurer la conciliation entre, d'une part, l'exercice de ces libertés constitutionnellement garanties et d'autre part, la prévention des atteintes à l'ordre public et notamment des atteintes à la sécurité des personnes et des biens qui répond à des objectifs de valeur constitutionnelle* » (Cons. const., décision n° 94-352, 18 janvier 1995, cons. 16).

d) la « *prévention de la criminalité et de la délinquance organisées* », qui figure au 6° de la disposition en cause. Si l'on s'accorde sans mal sur la nécessité de lutter contre ces formes de criminalité et de délinquance, la fin ne justifie pas tous les moyens, de sorte que l'atteinte qui en résulte pour le respect de la vie privée est excessive.

En effet, à l'instar de l'ensemble des droits et libertés que la Constitution garantit, le droit au respect de la vie privée peut faire l'objet de restrictions notamment au nom d'autres impératifs et droits constitutionnels. Toutefois, de telles restrictions doivent être « *justifié*[e]*s par un motif d'intérêt général et mis*[es] *en œuvre de manière adéquate et proportionnée à cet objectif* » (v. *mutatis mutandis* Cons. const., décision n° 2012-652 DC, 22 mars 2012, cons. 8).

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

À cela s'ajoute que pour le conseil constitutionnel, « *le législateur tient de l'article 34 de la Constitution, ainsi que du principe de légalité des délits et des peines, l'obligation de fixer lui-même le champ d'application de la loi pénale et de définir les crimes et délits en termes suffisamment clairs et précis. Cette exigence s'impose non seulement pour exclure l'arbitraire dans le prononcé des peines, mais encore pour éviter une rigueur non nécessaire lors de la recherche des auteurs d'infractions* » (Cons. const. n° 2004-492 DC, 2 mars 2004, cons. 5).

L'utilisation de tels procédés se caractérise manifestement, en ce qui concerne la prévention de la criminalité, par une « *rigueur non nécessaire* » en ce domaine et dès lors contraire à l'article 9 de la Déclaration des droits de 1789.

B) En ce qui concerne l'article L. 811-4 du code de la sécurité intérieure

Avec l'article L. 811-4, le législateur renvoie à un décret en conseil d'État le soin de désigner « *les services, autres que les services spécialisés de renseignement* » qui peuvent être autorisés à recourir aux techniques spéciales de renseignement, et de « *préciser, pour chaque service, les finalités mentionnées à l'article L. 811-3 et les techniques qui peuvent donner lieu à autorisation* ».

On voit ainsi que le législateur autorise, compte tenu du large pouvoir d'organisation qu'il concède à l'administration, une forme de dissémination du recours à des techniques qui devraient, en regard des atteintes à la vie privée qui en résultent, rester l'apanage de services spécialisés.

En outre, l'administration, dans le cadre de ce pouvoir d'auto-organisation qui lui est reconnu largement, peut déterminer lesquelles des finalités peuvent être poursuivies par ces services non spécialisés ainsi que les techniques qu'il leur sera loisible de mettre en œuvre. Dans la mesure où ces techniques portent une atteinte forte à la vie privée et présentent aussi la caractéristique de recueillir des informations sur des personnes étrangères à la cible des services de renseignement (ex : IMSI-catcher), le législateur aurait dû le préciser dans la loi.

On ne conçoit guère d'incompétence négative plus préjudiciable à la garantie des droits fondamentaux, alors même que ceux-ci sont placés, traditionnellement, sous la protection de la loi et que le conseil constitutionnel, comme il a été dit, considère qu'« *il appartient au législateur, en vertu de l'article 34 de la Constitution, de fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ;* […] *il lui appartient notamment d'assurer la conciliation entre, d'une part, la sauvegarde de l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la protection de principes et de droits de valeur constitutionnelle et, d'autre part, le respect de la vie privée et des autres droits et libertés constitutionnellement protégés* » (Cons. const., décision n° 2003-467 DC, 13 mars 2003, cons. 20).

C) En ce qui concerne l'article L. 821-1 du code de la sécurité intérieure

Cet article concerne l'autorisation de mise en œuvre des techniques de renseignement. Le législateur fait de l'avis de la commission nationale de contrôle des techniques de renseignement une garantie de leur mise en œuvre avant que le premier ministre, seul compétent à cette fin, décide de leur application dans un cas d'espèce.

Il importe à ce stade de mettre en évidence les points suivants.

Le renseignement, compte tenu des finalités mentionnées à l'article L. 811-3 précité, relève du champ de la police administrative (v. Cons. const., décision n° 2005-532 DC, 19 janvier 2006, cons. 5).

Il n'en reste pas moins que les techniques de renseignement en cause, en raison de leur caractère particulièrement intrusif, appellent des garanties qui doivent aller au-delà de celles qui encadrent habituellement la prérogative de police administrative.

Ces techniques mettent en effet en cause, de manière radicale, la liberté et le droit au respect de la vie privée, de sorte que l'on voie mal comment l'administration pourrait légitimement assurer un contrôle de l'utilisation de techniques qui sont à son avantage. Cela conduirait, au sens propre, à ce que soit en définitive mis en place un « État de police », sans que les garanties de séparation des pouvoirs les plus nécessaires soient instituées.
Celles-ci appellent

- soit l'intervention du juge judiciaire, de sorte que le conseil constitutionnel, prenant acte du caractère intrusif des techniques en cause et nonobstant la finalité préventive du renseignement, transposera dans ce domaine les garanties normalement applicables à la

procédure pénale,
- soit l'autorisation (et non simplement l'avis) de la commission nationale de contrôle des techniques de renseignement

Le conseil constitutionnel a, au demeurant, déjà suivi un tel raisonnement dans un cas qui n'est pas sans intérêt ici. S'agissant de la liberté de communication, le conseil a en effet censuré les dispositions de la loi du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet, en ce qu'elles ont conféré à une autorité administrative (même) indépendante le pouvoir de suspendre l'accès à Internet, alors que cette prérogative devait incomber au juge judiciaire :

« *Considérant que les pouvoirs de sanction institués par les dispositions critiquées habilitent la commission de protection des droits, qui n'est pas une juridiction, à restreindre ou à empêcher l'accès à internet de titulaires d'abonnement ainsi que des personnes qu'ils en font bénéficier ; que la compétence reconnue à cette autorité administrative n'est pas limitée à une catégorie particulière de personnes mais s'étend à la totalité de la population ; que ses pouvoirs peuvent conduire à restreindre l'exercice, par toute personne, de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile ; que, dans ces conditions, eu égard à la nature de la liberté garantie par l'article 11 de la Déclaration de 1789, le législateur ne pouvait, quelles que soient les garanties encadrant le prononcé des sanctions, confier de tels pouvoirs à une autorité administrative dans le but de protéger les droits des titulaires du droit d'auteur et de droits voisins ;* » (Cons. const., décision n° 2009-580 DC, 10 juin 2009, cons. 16).

Par ailleurs, dans sa décision *Géolocalisation* qui certes concerne des techniques de police judiciaire, mais qui ne sont pas sans rapport avec les techniques de renseignement, le conseil a jugé :

« *14. Considérant que le recours à la géolocalisation ne peut avoir lieu que lorsque l'exigent les nécessités de l'enquête ou de l'instruction concernant un crime ou un délit puni d'une peine d'emprisonnement d'au moins trois ans, s'agissant d'atteinte aux personnes, d'aide à l'auteur ou au complice d'un acte de terrorisme ou d'évasion, ou d'au moins cinq ans d'emprisonnement, s'agissant de toute autre infraction, ainsi qu'à des enquêtes ou instructions portant sur la recherche des causes de la mort, des causes de la disparition d'une personne ou des procédures de recherche d'une personne en fuite ;*

15. Considérant que le recours à la géolocalisation est placé sous la direction et le contrôle de l'autorité judiciaire ; » (Cons. const., décision n° 2014-693 DC, 25 mars 2014, cons. 14 et 15).

On en déduit *mutatis mutandis* que compte tenu de l'étendue des techniques de renseignement, de leurs caractéristiques et des atteintes qu'elles portent au droit au respect de la vie privée, il y a tout lieu de les soumettre à un régime garantissant une protection effective des droits des citoyens, ce que le législateur a manqué de faire.

Plusieurs points retiennent l'attention :

a) En premier lieu, la protection apportée par la consultation préalable de la Commission nationale de contrôle des techniques de renseignement, qui est une autorité administrative – fût-elle indépendante –, est très en-deçà du standard de protection constitutionnellement qui doit

être exigé en matière de renseignement.

Le conseil constitutionnel a en effet décidé que : « *si le législateur peut prévoir des mesures d'investigation spéciales en vue de constater des crimes et délits d'une gravité et d'une complexité particulières, d'en rassembler les preuves et d'en rechercher les auteurs, c'est sous réserve que ces mesures soient conduites dans le respect des prérogatives de l'autorité judiciaire, gardienne de la liberté individuelle, et que les restrictions qu'elles apportent aux droits constitutionnellement garantis soient nécessaires à la manifestation de la vérité, proportionnées à la gravité et à la complexité des infractions commises et n'introduisent pas de discriminations injustifiées ; qu'il appartient à l'autorité judiciaire de veiller au respect de ces principes, rappelés à l'article préliminaire du code de procédure pénale, dans l'application des règles de procédure pénale spéciales instituées par la loi* » (Cons. const., décision n° 2004-492 DC du 2 mars 2004, cons. 6).

Or, en l'occurrence, le recours aux techniques spéciales de renseignement, en particulier la collecte massive et non ciblée d'informations, relève exclusivement des services sans que l'autorité judiciaire soit, d'une manière ou d'une autre, en mesure d'exercer un contrôle quelconque sur le bien-fondé du recours à ces techniques avant qu'elles ne soient effectivement mises en œuvre.

Compte tenu tant de la nature de ces techniques que de leurs conséquences sur l'exercice des droits individuels, il y a là une atteinte à l'article 66 de la Constitution qui fait de l'autorité judiciaire la « *gardienne de la liberté individuelle* » ainsi qu'à l'article 16 de la Déclaration des droits, lesquels excluent que la liberté et le droit au respect de la vie privée soit entièrement placés sous le contrôle de l'administration.

En tout état de cause, à supposer même que les mesures litigieuses ne relèvent pas du champ de la liberté individuelle au sens de l'article 66 de la Constitution, d'autres droits et libertés constitutionnellement garantis peuvent imposer l'existence d'un contrôle juridictionnel, en lieu et place de celui-ci réalisé par une autorité administrative indépendante.

Ainsi, au titre de la liberté d'expression et de communication, le Conseil constitutionnel a-t-il censuré les dispositions de la loi du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, en ce qu'elles ont conféré à une autorité administrative – même si celle-ci était indépendante – le pouvoir de suspendre l'accès à internet, au motif que :

« *Les pouvoirs de sanction institués par les dispositions critiquées habilitent la commission de protection des droits, qui n'est pas une juridiction, à restreindre ou à empêcher l'accès à internet de titulaires d'abonnement ainsi que des personnes qu'ils en font bénéficier ; que la compétence reconnue à cette autorité administrative n'est pas limitée à une catégorie particulière de personnes mais s'étend à la totalité de la population ; que ses pouvoirs peuvent conduire à restreindre l'exercice, par toute personne, de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile ; que, dans ces conditions, eu égard à la nature de la liberté garantie par l'article 11 de la Déclaration de 1789, le législateur ne pouvait, quelles que soient les garanties encadrant le prononcé des sanctions, confier de tels pouvoirs à une autorité administrative dans le but de protéger les droits des titulaires du droit d'auteur et de droits voisins* » (Cons. const., décision n° 2009-580 DC, 10 juin 2009, cons. 16).

Dès lors, pour le Conseil constitutionnel, en raison tant de la protection constitutionnelle reconnue au droit à la liberté d'expression et de communication, que de la gravité de l'atteinte

que les mesures litigieuses sont susceptibles d'emporter, seule une juridiction peut être habilitée à édicter de telles mesures.

Il est d'ailleurs particulièrement révélateur que, dans cette décision du 10 juin 2009, le Conseil constitutionnel ait expressément souligné que la méconnaissance de la liberté constitutionnelle était acquise du seul fait qu'un tel pouvoir de suspension de l'accès à internet soit ainsi confié à une autorité administrative en lieu et place d'une juridiction. Et ce, « *quelles que soient les garanties encadrant le prononcé des sanctions* » et indépendamment même du fait que l'autorité concernée était une autorité administrative indépendante.

b) En deuxième lieu, la circonstance que la prérogative décisionnelle appartienne au premier ministre est contraire aux garanties minimales qui résultent de la Constitution.

Il suffit de rappeler, à cet égard, que selon le conseil constitutionnel, « *eu égard aux exigences de l'ordre public, le législateur peut prévoir la possibilité d'opérer des visites, perquisitions et saisies de nuit dans le cas où un crime ou un délit susceptible d'être qualifié d'acte de terrorisme est en train de se commettre ou vient de se commettre, à condition que l'autorisation de procéder auxdites opérations émane de l'autorité judiciaire, gardienne de la liberté individuelle, et que le déroulement des mesures autorisées soit assorti de garanties procédurales appropriées* » (Cons. const., décision n° 96-377 DC, 16 juillet 1996, cons. 17).

Les techniques mises en œuvre au titre du renseignement ne diffèrent pas de celles mentionnées ci-dessus. Elles sont encore plus attentatoires à la liberté et au droit au respect de la vie privée.

Ici encore, le législateur a enfreint les articles 66 de la Constitution et 16 de la Déclaration des droits de l'homme, ainsi que les articles 2 et 4 de la même Déclaration.

D) En ce qui concerne l'article L. 821-5-2 du code de la sécurité intérieure

Cet article exclut du recours aux techniques de renseignement les parlementaires, magistrats, avocats et journalistes à raison « *de l'exercice de son mandat ou de sa profession* ». *A contrario*, les professeurs d'université et les maîtres de conférences y sont inclus. Or, c'est méconnaître qu'ils ne peuvent, pas davantage que les premiers, faire l'objet d'une telle surveillance. Leur statut s'y oppose, en ce que le législateur ne peut, à peine de méconnaître la Constitution, porter atteinte à la « *garantie de l'indépendance des professeurs d'université* » et, plus généralement, des enseignants-chercheurs dont on sait qu'elle résulte d'un principe fondamental reconnu par les lois de la République (Cons. const., décision n° 83-165 DC, 20 janvier 1984, cons. 17 à 28).

Par ailleurs, une telle exclusion du recours aux techniques de renseignement visant directement les magistrats, avocats ou journalistes ne suffit aucunement à garantir une protection effective du droit au secret dont doivent bénéficier ces professions.

En effet, celles-ci bénéficient d'un droit constitutionnellement garanti au secret.

S'agissant d'abord du droit de l'avocat afin de garantir la confidentialité de ses échanges et correspondances avec ses clients ou ses confrères, il importe de relever que celui-ci repose tant sur le droit au respect de la vie privée protégé au titre de l'article 2 de la Déclaration des droits, que 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. const., décisions n^{os} 2006-535 DC, 30 mars 2006, cons. 24 ; 2011-214 QPC, 27 janvier 2012, cons. 5 et 6 ; et Cons. const.,

décisions n^{os} 2006-540 DC, 27 juillet 2006, cons. 11 ; 2012-247 QPC, 16 mai 2012, cons. 3, 5 à 7 ; Sur la confidentialité des entretiens avocat-client, v. not. Cons. const., décision n° 2003-484 DC, 20 novembre 2003, cons. 49 à 53).

Cette garantie constitutionnelle fait écho à la forte protection européenne accordée à la confidentialité des échanges entre avocats et clients (v. not. Cour EDH, *Anc.* 5^{e} Sect., 6 décembre 2012, *Michaud c. France*, Req. n° 12323/11, § 117-119 ; Article 4 de la directive de l'Union européenne 2013/48/UE du 22 octobre 2013).

S'agissant ensuite du droit au secret des sources d'information journalistiques, il s'agit de l'un des corollaires les plus essentiels de la liberté d'expression journalistique et qui est classiquement défini – 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* ». Or, en vertu tant de la liberté de communication des pensées et des opinions garantie par les dispositions de l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789, laquelle protège le libre débat public et la libre diffusion de l'information, que de l'article 34 de la Constitution relatif à « *la liberté, le pluralisme et l'indépendance des médias* », ce droit au secret des sources d'informations est constitutionnellement protégé.

En outre, un tel droit au secret bénéficie d'une forte reconnaissance au plan international et européen (v. not. Cour EDH, G.C. 27 mars 1996, *Goodwin c. Royaume-Uni*, Req. n° 17488/90, § 39 ; Cour EDH, G.C. 14 septembre 2010, *Sanoma Uitgevers B.V. c. Pays-Bas*, Req. n° 38224/03, § 88)

Or, malgré l'exclusion directe prévue à l'article L. 821-5-2 du code de la sécurité intérieure, le législateur a manqué d'assortir le dispositif litigieux des garanties légales aux fins d'éviter une atteinte indirecte à ces secrets, en particulier *via* la surveillance de personnes ayant des contacts professionnels avec les avocats ou les journalistes.

Faute d'autres mécanismes spécifiques de protection susceptible de faire efficacement obstacle à la révélation, par cette voie, d'une information à caractère secret dont un avocat ou un journaliste est le dépositaire, l'ensemble des garanties présentes au sein du droit français sont vidées de leur pertinence face à la mise en œuvre des techniques de renseignements.

Certes, nul ne peut contester qu'au-delà du seul code de la sécurité intérieure, d'autres dispositions législatives interdisent la révélation d'informations relevant du secret professionnel (v. not. l'article 226-13 du code pénal ; l'article 66-5, alinéa 1er, de la loi n° 71-1130 du 31 décembre 1971 ; l'article 100-5, alinéa 3, du code de procédure pénale ; 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).

Toutefois, ces différentes interdictions ne sont assorties d'aucune sanction pénale. Plus encore, compte tenu des insignes particularités des techniques de renseignement, l'ensemble des différentes garanties destinées à garantir le droit au secret professionnel sont parfaitement inapplicables et ineffectives dans un tel cadre.

En effet, et premièrement, les garanties légales existantes ont essentiellement pour vocation d'offrir une protection à ces secrets professionnels et à leurs dépositaires uniquement dans le cadre d'une procédure pénale (v. ainsi l'article 100-5, alinéas 3 et 4 et les articles 326, alinéa 2,

et 437, alinéa 2, du code de procédure pénale). Mais nulle protection n'existe donc pour des dispositifs administratifs tels que ceux prévus par les dispositions législatives contestées.

Deuxièmement, compte tenu des modalités particulières des techniques de renseignement, l'ensemble des dispositions légales protégeant le secret professionnel ne peut être mobilisé pour faire obstacle et réprimer d'éventuelles atteintes à ce secret du fait de ces techniques.

En particulier, 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, puisque ce sont les agents administratifs qui ont vocation à méconnaître le secret professionnel, sans que les dépositaires initiaux du secret ne puissent eux-mêmes s'y opposer.

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.

Au demeurant, de telles carences manifestes ne sauraient être compensées par les seuls dispositifs de contrôle et d'autorisation prévus *a priori*, ceux-ci étant pour l'essentiel assurés par des institutions administratives. Dès lors, la protection du secret professionnel, en particulier du droit au secret des sources d'informations journalistiques, n'est aucunement garantie puisque ce n'est pas « *un juge ou tout autre organe décisionnel indépendant et impartial* » qui exerce le 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).

E) En ce qui concerne les articles L. 831-1 et suivants du code de la sécurité intérieure

Ces articles portent sur l'organisation et les pouvoirs de la commission nationale de contrôle des techniques de renseignement (CNCTR). À supposer, compte tenu de ce qui a été dit plus haut, qu'il s'agisse là d'une garantie suffisante aux droits et libertés mis en cause par l'utilisation des techniques de renseignement qu'elle a pour objet de contrôler, cette commission ne présente pas les garanties requises pour être conforme à ces mêmes droits et libertés constitutionnels.

a) La CNCTR peut être facilement contourné. L'alinéa 2 de l'article L. 821-4 dispose que « Lorsque l'autorisation est délivrée après un avis défavorable de la Commission nationale de contrôle des techniques de renseignement, elle indique les motifs pour lesquels cet avis n'a pas été suivi. » Par ailleurs, l'article L 821-5 dispose qu' « En cas d'urgence absolue et pour les seules finalités mentionnées aux 1°, 4° et au a) du 5° de l'article L. 811-3, le Premier ministre, ou l'une des personnes déléguées mentionnées à l'article L. 821-4, peut délivrer de manière

exceptionnelle l'autorisation mentionnée au même article L. 821-4 sans avis préalable de la Commission nationale de contrôle des techniques de renseignement. Il en informe celle-ci sans délai et par tout moyen. »

b) Par ailleurs, la composition de la CNCTR prévue à l'article L.831-1 est insuffisante pour permettre aux membres de saisir les enjeux et de protéger ainsi la liberté des individus. Sur 9 membres, un seul est qualifié pour sa connaissance en matière de communications électroniques. Or les techniques de renseignement utilisés relèvent de beaucoup de champs scientifiques distincts (réseaux de communication, informatiques, mathématiques, analyse de bases de données) qui ne peuvent être correctement appréhendés par une seule personne qualifiée. C'est pourtant la seule CNCTR qui est habilitée à contrôler l'usage de ces techniques, notamment les « boîtes noires », conformément à ce qui est prévu dans la loi…
Par ailleurs, le pouvoir législatif n'est lui représenté que par deux sénateurs et deux députés, sur 9 membres…

c) Surtout, les pouvoirs de la CNCTR sont très insuffisants en ne permettent pas de garantir le droit au respect de la vie privée. En particulier, il résulte de la combinaison des articles L. 833-3 al. 2, L. 833-3-2 et L. 833-3-4 qu'en cas d'irrégularité dans la mise en œuvre d'une technique de renseignement, rien ne garantit que les données conservées – illégalement – ne soient pas utilisées dans le cadre d'une procédure pénale, de même que la CNCTR ne peut en obtenir la destruction effective afin d'éviter toute atteinte subséquente au droit au respect de la vie privée qui viendrait s'ajouter à l'irrégularité de la collecte des données en cause.

Pour toutes ces dispositions, les signataires de cette saisine demandent au conseil constitutionnel de juger cette disposition comme allant à l'encontre de l'article 16 de la déclaration des droits de l'homme et du citoyen qui énonce le principe de la séparation des pouvoirs, principe à valeur constitutionnelle ayant pour finalité de garantir la liberté des individus.

2°) SUR L'ARTICLE 2

A) En ce qui concerne les articles L. 851-1 et L. 851-3 du code de la sécurité intérieure

Au titre des « Des techniques de recueil de renseignement soumises à autorisation » l'article L. 851-1 permet le recueil, auprès d'opérateurs et d'hébergeurs, d'informations ou de documents portant sur les communications électroniques [v. l'opportunité d'élargir la critique à l'article L. 851-3].

a) Premièrement, il importe de souligner que le législateur s'est abstenu de définir les notions d'« *informations et documents* » susceptibles d'être recueillis par les autorités administratives.

Ainsi, les critiques qui ont été émises envers les dispositions de l'article L. 246-1 du code de la sécurité intérieure, initialement issues de 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 désormais reprises au sein de l'article L. 851-1, n'ont aucunement perdu de leur pertinence :

« *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 ; v. aussi 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).

A propos de ces mêmes dispositions, la doctrine n'a pas non plus manqué de mettre en exergue cette insuffisance définitionnelle :

« *La formulation retenue par le projet de loi de programmation miliaire vise non seulement les données de connexion, mais encore beaucoup plus largement les informations et documents stockes 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 Duhen, « L'imbroglio 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* »).

Dès lors, en s'abstenant d'assortir la définition de la notion d'« *informations ou documents* » de « *limitations et précautions* » requises par le conseil constitutionnel (Cons. const., décision n° 2005-532 DC, 19 janvier 2006, cons. 10), le législateur a nécessairement autorisé « *la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel* » (Cons. const., décision n° 2012-652 DC, 22 mars 2012, cons. 8) sans prévoir « *les garanties appropriées et spécifiques répondant aux exigences de l'article 34 de la Constitution* » (Cons. const., décision n° 2004-499 DC, 29 juillet 2004, cons. 11).

Plus précisément encore, le législateur a « *privé de garanties légales des exigences constitutionnelles* » (Cons. const., décisions n°s 2012-652 DC, 22 mars 2012, cons. 7 et 2004-499 DC, 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.

Ainsi, non seulement ces « *informations ou documents* » peuvent nécessairement aller au-delà des seules données de connexion et viser le contenu même des communications électroniques. Mais en outre, faute de définition légale univoque, les dispositions litigieuses en viennent nécessairement à « *faire dépendre le champ d'application* » des techniques de recueil de renseignement, en soi particulièrement intrusives et attentatoires 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. const., décision n° 98-399 DC, 5 mai 1998, cons. 7).

b) Deuxièmement, les finalités qui justifient un tel accès ayant connu un élargissement

sensible et, à ce titre, hautement contestable, une telle prérogative porte nécessairement une atteinte disproportionnée au droit au respect de la vie privée.

Le conseil constitutionnel s'est d'ailleurs montré pour le moins sensible à cet égard, puisqu'il a considéré, au sujet de la modification de l'article 9 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés par la loi du 29 juillet 2004, que :

« *11. Considérant que le 3° de l'article 9 de la loi du 6 janvier 1978, dans la rédaction que lui donne l'article 2 de la loi déférée, permettrait à une personne morale de droit privé, mandatée par plusieurs autres personnes morales estimant avoir été victimes ou être susceptibles d'être victimes d'agissements passibles de sanctions pénales, de rassembler un grand nombre d'informations nominatives portant sur des infractions, condamnations et mesures de sûreté ; 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 ; que la disposition critiquée doit dès lors comporter les garanties appropriées et spécifiques répondant aux exigences de l'article 34 de la Constitution ;*

*12. Considérant que, 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 négativ*e » (Cons. const., décision n° 2004-499 DC, 29 juillet 2004, cons. 11 et 12).

En l'occurrence, compte tenu de l'ampleur des techniques de recueil de renseignement, la procédure particulière suivie devant la CNCTR n'est pas suffisante pour que la conciliation entre l'ordre public et le droit au respect de la vie privée soit conforme à la Constitution.

c) Troisièmement, **les documents mentionnés à l'article 2 (L851-1, L851-3, L851-4 et sq) ont été qualifiés par le gouvernement, tout au long des débats parlementaires, comme des « méta-données ».**

La définition du dictionnaire Larousse est la suivante : Donnée servant à caractériser une autre donnée, physique ou numérique : les métadonnées sont à la base de l'archivage.
En réalité, il n'existe pas de définition juridique des métadonnées. On l'entend donc de manière « empirique » comme l'ensemble des informations qui concernent la donnée. [LAURE : A COMPLETER EN ANNEXE car il existe une définition juridique de la métadonnée par décret]
Concrètement, prenons une lettre. La donnée serait le contenu de la lettre, et les métadonnées, l'ensemble des informations s'y rapportant : la couleur et la taille de l'enveloppe, le lieu et l'heure à laquelle elle a été postée, celle où elle a été reçue par le centre de tri, mais si l'on va

plus loin, ce peut également être le lieu où l'enveloppe a été achetée, avec quelle carte de crédit, l'acheteur l'a payé, etc…

Dans le cadre d'un appel téléphonique, les métadonnées auxquelles on pense naturellement sont donc l'heure et la durée de l'appel, l'identifiant de l'appelant et de l'appelé, ou encore la borne de réception utilisée. Mais il existe d'autres métadonnées tout aussi intéressantes pour les services de renseignement, qui peuvent être concernées par cette définition imparfaite de l'article L 851-1. On peut rechercher le type d'abonnement, les problèmes de paiement, les différentes adresses du souscripteur du contrat…

Dans le cas d'une connexion internet, les métadonnées sont très souvent plus informatives que le contenu d'un message.

Or, les défenseurs du texte ont avancé durant les débats, l'idée que les données relatives aux contenus étaient moins intrusives que le contenu lui-même, et ne permettait pas l'identification d'une personne. Ils disaient que cela permettait l'anonymat des données collectées.

Cette conception, qui était recevable du temps des seules écoutes sur des téléphones fixes, est aujourd'hui parfaitement dépassée.

Tous les experts confirment que la collecte des métadonnées permette parfaitement d'identifier une personne et que l'analyse des métadonnées en dit autant, voire plus que le contenu même des échanges.

Exemple : recueillir les métadonnées d'une femme qui se rend sur des sites pour les femmes souffrant d'un cancer du sein, qui écrit un courriel à son médecin, qui lui répond, puis recherche le numéro d'un centre de radiologie à proximité de son domicile, donne des informations très personnelles sur cette femme. Il y a fort à parier que cette femme pense souffrir d'un cancer du sein, qu'elle en a informé son médecin, et qu'elle souhaite aller faire une radiographie pour s'en assurer…

Il n'est pas nécessaire de regarder le contenu précis de l'échange qu'elle a eu avec son médecin pour avoir la quasi-certitude que cette femme pense souffrir d'un cancer du sein. Les seules métadonnées ont suffi.
Prenons aussi l'exemple d'une personne qui consulterait des sites libertins ou échangistes, ou consulterait des sites religieux ou politiques, sans que jamais, au cours d'aucune conversation, il n'évoque cette habitude… Le mode de consommation d'Internet (métadonnées) en dit plus sur certains centres d'intérêt de cette personne que le contenu même de ses conversations.

En outre, le traitement des métadonnées est beaucoup plus rapide et aisé que le traitement des contenus. Déduire du traitement d'un contenu (image ou texte) le même nombre d'informations qu'offrent les métadonnées est donc illusoire.

Ainsi, les métadonnées sont bien plus intrusives et portent davantage atteinte à la vie privée que les contenus eux-mêmes.

Enfin, les derniers développements techniques vont jusqu'à remettre en cause la distinction entre métadonnées et contenu.

Or, l'article 2 de la Déclaration des droits de l'Homme et du citoyen du 26 août 1789 implique

le respect de la vie privée, comme l'a affirmé le Conseil constitutionnel à plusieurs occasions, et notamment dans une décision du 23 octobre 1990 rendu par la Première Chambre Civile de la Cour de Cassation : « toute personne, quels que soient son rang, sa naissance, sa fortune, ses fonctions présentes ou à venir, a droit au respect de sa vie privée. »

Ce principe a été réaffirmé dans une décision n° 94-352 DC du 18 janvier 1995 dans laquelle il indiquait que : « Considérant que la prévention d'atteintes à l'ordre public, notamment d'atteintes à la sécurité des personnes et des biens, et la recherche des auteurs d'infractions, sont nécessaires à la sauvegarde de principes et droits à valeur constitutionnelle ; qu'il appartient au législateur d'assurer la conciliation entre ces objectifs de valeur constitutionnelle et l'exercice des libertés publiques constitutionnellement garanties au nombre desquelles figurent la liberté individuelle et la liberté d'aller et venir ainsi que l'inviolabilité du domicile ; que la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle »

A la lecture de cette décision, il convient de s'interroger sur l'existence d'une proportionnalité entre cette violation de la vie privée via la collecte massive de métadonnées sur des personnes totalement étrangères à la cible recherchée par les services de renseignement, prévue notamment à l'article 2 (mais aussi à l'article 3 et suivants) et les objectifs de sécurité des personnes et des biens poursuivis par le projet de loi.

B) En ce qui concerne l'article L. 851-4 du code de la sécurité intérieure

Cet article porte sur la mise en place de « boîtes noires algorithmiques » et constitue manifestement une mesure contraire aux droits et libertés constitutionnels. Quand bien même le législateur a précisé dans le second alinéa de cet article que les traitements automatisés dont s'agit ne permettent pas « *l'identification des personnes auxquelles les informations ou documents se rapportent* », une telle garantie est illusoire car l'identification découle *in fine* de la nature de ces données.

Techniquement, cet article (et le précédent L851-3) visent à rendre obligatoire l'installation de boîtes noires algorithmiques sur les réseaux des opérateurs de télécommunication situés sur le territoire national.

Les services de renseignement seront habilités à recevoir l'ensemble des informations transitant par ces infrastructures afin de pouvoir détecter grâce à des algorithmes, des terroristes et leurs soutiens parmi la masse des internautes.

Le texte prévoit de repérer des « signaux faibles », en comparant les activités en ligne de terroristes connus avec l'activité quotidienne de l'ensemble de la population. La nature de ces dispositifs est de détecter les comportements considérés comme « anormaux » par les concepteurs desdits « algorithmes ». On espère repérer ainsi ceux qui se cachent dans la masse. Ces équipements sont indubitablement des équipements de surveillance de masse, puisqu'ils ont vocation à analyser l'ensemble du trafic qui transite par eux, de façon indiscriminée.

Or, non seulement ce dispositif est disproportionné par rapport aux risque d'atteinte à la vie privée ; mais il est également totalement inefficace.

Un certain nombre d'experts, et notamment ceux de l'INRIA, institut national de référence dans les sciences du numérique ont démontré le peu de pertinence d'un tel outil, et la surveillance de masse qu'il autorisait. Cf note de l'INRIA ci-jointe.

La principale cause d'inefficacité de ces dispositifs est qu'ils génèrent trop de « faux positifs », c'est-à-dire considèrent à tort des individus comme suspects. En supposant, de façon très optimiste, un taux de 1 % de faux positifs, cela représenterait, à l'échelle du pays, près de 500.000 personnes, contre près de 2.500 personnes que l'on voudrait cibler, soit un taux de réussite inférieur à 0,5 %.
Or les chercheurs de l'INRIA indiquent que les algorithmes prédictifs des comportements humains donnent aujourd'hui plutôt 99% de faux positifs.

Il s'agit donc en fait de mettre en œuvre une version numérique et aseptisée de « loi sur les suspects », comme ont pu en connaître les périodes les plus sombres de notre histoire. Rappelons que ces lois furent à chaque fois abrogées, au vu de leur inefficacité et des «dommages collatéraux » qu'elles ont occasionnés au sein de la population.

Considérer au moins 1 % de la population comme suspecte, c'est faire en sorte que chacun de nous connaisse, parmi sa famille ou ses relations, au moins un suspect, sinon plusieurs. C'est instaurer une suspicion numérique généralisée.

Les Etats-Unis, qui avaient mis en place ce type de programmes, dans le cadre du Patriot Act, ont tiré un constat d'échec du dispositif dans la lutte contre le terrorisme. Au lieu de renouveler le Patriot Act pour quatre années supplémentaires, le Congrès américain a souhaité faire passer une nouvelle loi, le Freedom Act, censé mettre un terme à la collecte massive de données par la NSA.

Il semble bien plus pertinent d'attribuer les moyens envisagés pour ce programme au renseignement humain et aux surveillances ciblées. Il ne faut pas oublier que les auteurs des attentats commis en France en 2012 et en 2015 étaient clairement identifiés par les services de renseignements, et que faute de moyens humains, il n'a pas été possible d'opérer une surveillance suffisante permettant d'anticiper leurs passages à l'acte.

La disproportion qui existe entre cette surveillance de masse et l'intérêt qu'elle représente dans le cadre de la lutte pour la sécurité des personnes et des biens est flagrante et contrevient aux principes énoncés à l'article 2 de la Constitution.

Comme énoncé précédemment, ces boîtes noires algorithmiques traitent de manière indifférenciée toutes les données traitées par les réseaux et cela inclut nécessairement des données à caractère personnel.

Il y a là une atteinte manifeste au droit au respect de la vie privée qui ne peut être justifiée par la sauvegarde de l'ordre public. Et cela d'autant plus que le conseil constitutionnel apprécie l'atteinte inconstitutionnelle à ce droit à l'aune des garanties prévues par la loi.

À cet égard, il a été jugé que « *la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle* » et que « *la mise en œuvre de systèmes de vidéosurveillance doit être assortie de garanties protectrices de son exercice* ». (Cons. const., décision n° 94-352 DC, 18 janvier 1995, cons. 3 et 4).

Par ailleurs, le conseil constitutionnel a décidé, « *eu égard, d'une part, aux garanties apportées par les conditions d'utilisation et de consultation du fichier judiciaire automatisé des auteurs d'infractions sexuelles et par l'attribution à l'autorité judiciaire du pouvoir d'inscription et de retrait des données nominatives, d'autre part, à la gravité des infractions justifiant l'inscription des données nominatives dans le fichier et au taux de récidive qui caractérise ce type d'infractions, les dispositions de l'article 48 de la loi portant adaptation de la justice à l'évolution de la criminalité sont de nature à assurer, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée* » (Cons. const., décision n° 2004-492 DC, 2 mars 2004, cons. 87 et 88).

Enfin, il a considéré que « *eu égard aux finalités du casier judiciaire, elle ne saurait, sans porter une atteinte non nécessaire à la protection de la vie privée qu'implique l'article 2 de la Déclaration de 1789, être mentionnée au bulletin n° 1 du casier judiciaire que lorsque des mesures de sûreté ont été lorsque des mesures de sûreté prévues par le nouvel article 706-136 du code de procédure pénale ont été prononcées et tant que ces interdictions n'ont pas cessé leurs effets* » (Cons. const., décision n° 2008-562 DC, 21 février 2008, cons. 31).

L'atteinte au droit au respect de la vie privée est d'autant plus forte que le législateur n'a assorti l'article en cause d'aucune disposition venant garantir un traitement proportionné des « faux positifs » statistiques.

Aussi bien, en l'absence de toute garantie adéquate permettant d'éviter, notamment, les conséquences arbitraires d'une simple erreur ou d'un calibrage insuffisant des algorithmes, l'article dont s'agit est contraire à la Constitution.

C) En ce qui concerne les articles L. 851-5, L. 851-6, L. 851-7 du code de la sécurité intérieures

Ces articles ont trait à différentes techniques de renseignement qui portent une atteinte disproportionnée au droit au respect de la vie privée compte tenu du caractère vague des finalités qui justifient leur mise en œuvre. Ils sont donc également contraires car disproportionnés à l'article 2 de la Déclaration des droits de 1789.

D) En ce qui concerne l'article L. 852-1 du code de la sécurité intérieure

Cet article autorise les interceptions de correspondances émises par la voie des communications électroniques et susceptibles de révéler des renseignements relatifs aux finalités mentionnées à l'article L. 811-3.

[Même critique que précédemment]

3°) SUR L'ARTICLE 3

A) En ce qui concerne les articles L. 853-1 à L. 853-3 du code de la sécurité intérieure

La surveillance des communications par les extrémités nuit gravement à l'inviolabilité du domicile. C'est le cas de l'installation des logiciels espions permise par le 2 de l'article 853-2

De nos jours, il est très facile d'installer, sur son ordiphone et/ou son ordinateur, des logiciels

gratuits et fiables de chiffrement des communications électroniques, qui garantissent « de bout en bout » la confidentialité de celles-ci.

Ces outils cryptographiques sont utilisés tant par les criminels que par les industriels et les simples citoyens désireux d'échapper aux programmes de surveillance massive mis en place par certains régimes, démocratiques ou non. Face à de tels outils, les services de police sont démunis, car toute interception réalisée en dehors du domicile ne permet que d'avoir accès au flux chiffré, impossible à décrypter par les technologies actuelles.

Le seul moyen pour les services consiste donc à intercepter ces flux avant qu'ils ne soient chiffrés, c'est-à-dire en les capturant à la source sur l'ordinateur de l'un des participants. C'est pour cela qu'ont été incluses au projet de loi, au 2° de l'article L. 853-2, des dispositions permettant l'installation, sur les ordinateurs des suspects, de logiciels espions chargés d'intercepter les frappes au clavier et/ou les flux audio et vidéo issus des différents périphériques de l'ordinateur.

Cependant, rien n'empêche, une fois ces dispositifs installés, qu'ils puissent être utilisés alors qu'une communication n'est pas en cours. Le recueil des frappes au clavier permet alors de connaître ce que la personne écrit dans son journal intime, et le micro et la caméra de l'ordinateur captent l'ambiance du domicile pourtant réputé inviolable.
Ainsi, il faut bien comprendre que l'utilisation de ces logiciels espions peut aboutir à deux situations juridiques différentes :

- s'il est utilisé pour écouter par exemple ce que la personne va transmettre volontairement via son ordinateur (une conversation sur Skype par exemple) : juridiquement, cette interception n'est pas considérée comme une sonorisation du domicile.
- s'il est utilisé de manière continue avec un branchement de caméra qui intercepte tout ce qui se passe dans l'environnement de la pièce : juridiquement c'est de la sonorisation de domicile.
  Or, cette deuxième finalité est expressément organisée par l'article L. 853-1.

Il est donc essentiel qu'un horodatage précis des transmissions de flux soit effectué, afin que ces dispositifs ne puissent pas être utilisés en dehors de la captation de communications. Cela impose que les logiciels d'interception intègrent les fonctionnalités permettant de prendre en compte cette problématique, et n'activent la capture des différents périphériques que lorsqu'ils sont effectivement employés dans le cadre d'une conversation avec un correspondant extérieur au domicile.

Aujourd'hui, on ne peut techniquement différencier les deux actions.

Le « débridage » de ces outils pour réaliser la « sonorisation » d'un domicile doit être encadré de la même façon que la mise en œuvre de dispositifs d'écoute traditionnels ; au vu de son très fort niveau d'intrusion, l'accord d'un juge judiciaire semble absolument nécessaire.

Aussi, par principe, il faut appliquer le régime le plus protecteur en matière de liberté publique, c'est-à-dire rendre la saisine du juge obligatoire avant toute implantation de logiciel espion.

En effet, depuis 1999, en effet, le Conseil constitutionnel, considère le droit au respect de la vie privée comme une composante de la liberté personnelle proclamée à l'article 2 de la Déclaration des droits de l'homme et du citoyen, dont résultent également le droit au secret des

correspondances et le principe de l'inviolabilité du domicile.

Dans sa décision du 2 mars 2004 relative à la loi portant adaptation de la justice aux évolutions de la criminalité, le Conseil constitutionnel a invoqué les articles 2 et 4 de la Déclaration de 1789 en considérant qu'« il incombe au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des libertés constitutionnellement garanties ; qu'au nombre de celles-ci figurent la liberté d'aller et venir, l'inviolabilité du domicile privé, le secret des correspondances et le respect de la vie privée, protégés par les articles 2 et 4 de la Déclaration de 1789 ».

En l'espèce, l'atteinte à l'inviolabilité du domicile privé est avérée, et non proportionnée aux risques d'atteintes à l'ordre public. Par ailleurs, l'absence totale d'un contrôle du juge judiciaire vient renforcer cette violation de l'article 2 de la déclaration des droits de l'homme et du citoyen, et des principes en découlant.

B) En ce qui concerne l'article L. 854-1 du code de la sécurité intérieure

Cet article concerne les mesures de surveillance internationale que les autorités françaises sont habilitées à mettre en œuvre, lorsque les communications sont émises ou reçues en dehors du territoire national.

Le législateur met ainsi en place une possibilité de surveillance généralisée et non contrôlée, puisqu'il est énoncé à l'article L. 833-2 que pour l'accomplissement de ses missions, la commission : « *2° Dispose d'un accès permanent, complet et direct aux relevés, registres, renseignements collectés, transcriptions et extractions mentionnés au présent livre, à l'exception de ceux mentionnés à l'article L. 854-1* ».

Ici encore, l'atteinte au droit au respect de la vie privée est manifestement excessive en l'absence de garanties qui sont, lorsqu'elles existent, insuffisantes.

4°) REMARQUES TRANSVERSES SUR LA COLLECTE DES DONNÉES ET SUR LA DUREE DE CONSERVATION DES DONNÉES

a) Collecte des données des personnes totalement étrangères à l'enquête par l'utilisation des «*IMSIcatcher »*

Le rôle des IMSIcatcher mentionnés à l'article L 851-7 III° est de simuler le fonctionnement d'une borne relais de réseau de téléphone mobile, afin d'intercepter tous les appels des téléphones mobiles environnants se connectant à cette borne. Il s'agit donc bien d'une interception de masse, indiscriminée. Comme pour une borne-relai, les captations des IMSIcatchers ne concernent que l'ensemble des téléphones situés à proximité, et non pas seulement le téléphone de la personne visée par l'enquête.

Un premier point à noter est que, pour que l'interception des contenus des conversations soit possible, l'*IMSIcatcher* doit exclusivement mettre en oeuvre une ancienne version du protocole de communication entre téléphones mobiles et borne relais. Cette ancienne version, à la différence des suivantes, ne chiffre pas les informations transmises. En prétendant ne disposer que de ce protocole non chiffré, la borne *IMSIcatcher* impose aux téléphones environnants de ne pas chiffrer leurs contenus lorsqu'ils s'adressent à elle. Ceci induit donc une faille de sécurité dans toutes les communications passant par l'*IMSIcatcher*, puisque n'importe qui peut alors intercepter en clair les communications échangées. De fait, si le projet de loi prétend protéger certaines professions (parlementaires, journalistes, avocats notamment), elle dégrade le niveau de sécurité de leurs communications et les rend vulnérables à toute interception.

La collecte indifférenciée des conversations à portée d'un *IMSIcatcher* est potentiellement nuisible à de nombreuses catégories de personnes protégées par la loi (avocats, magistrats, journalistes, etc.), ainsi qu'à leurs sources. Qui plus est, si une telle collecte de masse est considérée comme illégale sur l'ensemble d'un territoire, rien ne peut non plus la justifier au sein d'une fraction de ce territoire…

C'est également pour contourner le chiffrement mis en œuvre par les nouvelles versions des protocoles 3G et 4G que le GCHQ et la NSA ont fait intrusion au sein des serveurs de la société Gemalto, et ont pu siphonner les clés de chiffrement des cartes SIM de plusieurs millions d'usagers.

Si l'utilité des *IMSIcatcher* n'est pas remise en cause, leur conception et leur mise en oeuvre doivent être fortement encadrées. Ainsi, ces dispositifs devraient être bridés par conception afin de ne pouvoir restituer à leurs opérateurs que les communications issues d'une liste mémorisée de numéros de téléphones, aucune des autres conversations ne pouvant être retranscrite. Si l'ajout des numéros de téléphone peut se faire « à la volée », pour suivre certaines conversations, l'horodatage de ces ajouts (et suppressions) doit pouvoir être une pièce opposable en justice, afin de justifier qu'une interception téléphonique n'a pas eu lieu au moyen d'un appareil «débridé», mais bien de façon ciblée, pour des motifs devant être portés aux rapports des missions d'interception. La responsabilité des fabricants doit être engagée sur l'absence de «portes dérobées» permettant de « débrider » temporairement et secrètement ces appareils.
Des dispositions relatives à l'homologation de ces dispositifs devraient donc être introduites au sein du projet de loi, définissant de façon explicite les limitations que le législateur entend appliquer à ces dispositifs. Les modalités d'homologation pourraient, pour leur part, être spécifiées de façon réglementaire.

b) Durée de conservation des données et méta-données

L'article 1er du projet de loi dispose :

(…) Art. L. 822-2. – I. – Les renseignements collectés par la mise en œuvre d'une technique de recueil de renseignement autorisée en application du chapitre Ier du présent titre sont détruits à l'issue d'une durée de :

« 1° Trente jours à compter de leur recueil pour les correspondances interceptées en application de l'article L. 852-1 et pour les paroles captées en application de l'article L. 853-1 ;

« 2° Cent vingt jours à compter de leur recueil pour les renseignements collectés par la mise en œuvre des techniques mentionnées au chapitre III du titre V du présent livre, à l'exception des informations ou documents mentionnés à l'article L. 851-1 ;

« 3° Quatre ans à compter de leur recueil pour les informations ou documents mentionnés à l'article L. 851-1.

« Pour ceux des renseignements qui sont chiffrés, le délai court à compter de leur déchiffrement. Ils ne peuvent être conservés plus de six ans à compter de leur recueil.

« Dans une mesure strictement nécessaire aux besoins de l'analyse technique et à l'exclusion de toute utilisation pour la surveillance des personnes concernées, les renseignements collectés qui contiennent des éléments de cyberattaque ou qui sont chiffrés, ainsi que les renseignements déchiffrés associés à ces derniers, peuvent être conservés au-delà des durées mentionnées au présent I.

« II et III. – (Supprimés)

« IV. – Par dérogation au I du présent article, les renseignements qui concernent une requête dont le Conseil d'État a été saisi ne peuvent être détruits. À l'expiration des délais prévus au même I, ils sont conservés pour les seuls besoins de la procédure devant le Conseil d'État. (…)

Lors du vote de la loi relative à la lutte contre le terrorisme et portant diverses mesures relatives à la sécurité routière et aux contrôles frontaliers, (décision n°2005-532 DC du 19 janvier 2006) le Conseil constitutionnel a validé le principe suivant :

Considérant que les enregistrements seront effacés au bout de huit jours si les caractéristiques permettant l'identification des véhicules, ainsi collectées, ne figurent ni dans le fichier national des véhicules volés ou signalés, ni dans la partie du système d'information Schengen relative aux véhicules ; que les critères de cette recherche seront les caractéristiques des véhicules et non les images des passagers ; que les données n'ayant pas fait l'objet d'un " rapprochement positif " ne pourront être consultées pendant ce délai, sous réserve des besoins résultant d'une procédure pénale ; que seules les données ayant fait l'objet de ce rapprochement seront conservées ; que la durée de cette conservation ne pourra alors excéder un mois, sauf pour les besoins d'une procédure pénale ou douanière ; que seuls auront accès au dispositif, dans les limites ci-dessus décrites, des agents des services de la police et de la gendarmerie nationales

individuellement désignés et dûment habilités ; que les traitements automatisés des données recueillies seront soumis aux dispositions de la loi du 6 janvier 1978 susvisée ;

Cette décision peut être interprétée comme validant la conservation de donnée pour une durée indéterminée si elles sont nécessaires aux besoins d'une procédure pénale ou douanière.

Néanmoins, dans le communiqué de presse publié consécutivement à cette décision, il est précisé que :

Le 19 janvier 2006 (décision n° 2005-532 DC), le Conseil constitutionnel a statué sur la loi " relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers " dont il avait été saisi par plus de soixante sénateurs.

Ceux-ci en contestaient l'article 6 (réquisition administrative de "données de trafic" auprès d'opérateurs de communications électroniques, de fournisseurs de services en ligne et de "cyber-cafés"), ainsi que l'article 8 (photographie automatique des véhicules et de leurs occupants sur certains axes routiers et enregistrement provisoire de ces photographies aux fins de rapprochement avec les fichiers de véhicules volés ou signalés)
.
Le Conseil constitutionnel n'a pas déclaré ces dispositions contraires à la Constitution eu égard, d'une part, à leur utilité dans la lutte contre le terrorisme et la criminalité, d'autre part, aux limitations et précautions dont elles étaient assorties du point de vue de la protection de la vie privée.

En 2006, le Conseil constitutionnel a donc validé le principe de la conservation des données, estimant que les garanties étaient réunies, et donc le principe de proportionnalité respecté, entre lutte contre le terrorisme et la criminalité d'un côté, et l'atteinte à la vie privée de l'autre.

Mais nous sommes dans un contexte tout autre que celui de la décision de 2006 du Conseil Constitutionnel.
En premier, nous avons préalablement démontré que les moyens mis en œuvre permettant la collecte de données dans le projet de loi faisant l'objet de cette saisine, sont massifs, peu clairs et inadaptés par rapport aux objectifs poursuivis.

En second, l'atteinte à la vie privée que peut représenter la collecte et la conservation de données est bien supérieure à ce qu'elle pouvait être en 2006, lors de la décision précitée.

En 2006, l'accès à Internet n'était pas utilisé à chaque moment de notre vie. Aujourd'hui, on ne se connecte plus, on est connecté en permanence à Internet !

Le taux d'équipement en smartphone était négligeable, et cette technologie quasi confidentielle en France était réservée à un usage professionnel. Les temps de connexion étaient beaucoup plus longs, les appareils nettement moins simples d'utilisation et quasiment limités à l'envoi/réception de courriels.

Dans une étude datée de juin 2014, réalisée par la Mobile Marketing Association (MMA) France, un Français sur deux possède un smartphone (soit 27,7 millions de Français) et un foyer sur trois est équipé d'au moins une tablette (soit 9,1 millions de foyers). 75% des Français ont accès à Internet haut débit chez eux. En outre, trois téléphones mobiles sur quatre vendus en 2014 seront des smartphones (soit 17,5 millions d'unités).

65,2% des français devraient être équipés d'un smartphone en 2017, estime eMarketer[1].

Dans les années qui viennent, ce ne seront plus simplement les « smartphones » ou les tablettes qui seront connectés, mais l'ensemble des objets qui nous entourent : montres, téléviseurs, réfrigérateurs, robots ménagers, …

Aussi, la progression du taux d'équipement et des usages entre 2006 (date de la décision du conseil constitutionnel) et 2015 vient considérablement augmenter le nombre de données susceptibles d'être recueillies, traces de chaque instant de notre vie personnelle et privée.

Aujourd'hui, l'espace intime reste préservé des données susceptibles d'être interceptées. Mais demain, lorsque votre téléviseurs sera connecté et capable d'analyser votre conversation pour vous aider dans votre quotidien. Ce seront autant d'informations susceptibles d'être recueillies dans le cadre de l'application de cette loi.

Prenons l'exemple d'un couple qui discute d'un futur voyage en Jordanie. Le téléviseur sera en mesure de leur proposer immédiatement des offres de vols et de circuits touristiques pour cette destination. Et les boîtes noires des opérateurs, d'enregistrer la consultation de sites de voyages vers la Jordanie.

Dans cette hypothèse, les comportements privés ne risquent-ils pas d'être affectés par le risque encouru d'atteinte à la vie privée ? La surveillance de masse autorisée par ce texte n'est-elle pas de nature à restreindre la liberté d'action et de parole de tout à chacun ? Et qu'en sera-t-il lorsque des données beaucoup plus précises seront disponibles en matière de santé par exemple ?

Le champ d'habilitation très large permettant de récolter des informations, et le nombre considérable de données susceptibles d'être collectées entraîne une disproportion flagrante entre les moyens mis en œuvre en matière de sécurité des personnes et des biens, et la masse de conservation de données personnelles portant ainsi atteintes au respect de la vie privée.

Le gouvernement a d'ailleurs bien conscience de la difficulté de rendre conforme à la Constitution la conservation de données cryptées puisque le Premier Ministre, lors de son audition devant la commission des lois du Sénat, a parlé de conservation de données anonymes ». Ce terme est un non-sens technique, puisque la captation des données n'est pas anonyme, que les métadonnées permettent d'identifier les individus et et que la conservation de données cryptées anonyme n'aurait aucun intérêt.

Aussi, l'article 1er, 2 et 3 du projet de loi est contraire à l'article 2 de la Constitution, en ce qu'il porte atteinte au respect de la vie privée et à la liberté d'expression. Il doit donc à ce titre être censuré.

5°) SUR L'ARTICLE 4

En ce qui concerne les articles L. 773-1 à L. 773-8 du code de justice administrative

[1] http://www.cbnews.fr/etudes/plus-de-la-moitie-des-francais-possederont-un-smartphone-en-2015-a109906

Ces articles définissent les modalités du contrôle juridictionnel a posteriori du recours aux techniques de renseignement. En faisant la part belle au secret défense, les règles applicables à cette voie de droit ouverte devant le conseil d'État méconnaissent une exigence pourtant inhérente à toute procédure contentieuse : le respect du contradictoire.

Celui-ci ne semble pas disparaître, puisque l'article L. 773-3 du code de justice administrative énonce : « *Les exigences de la contradiction mentionnées à l'article L. 5 sont adaptées à celles du secret de la défense nationale* ».

Mais cette adaptation n'en est pas vraiment une, puisque tout contradictoire est purement et simplement évacué de la procédure en question.

La procédure est en effet tout sauf équitable : le requérant ne sait pas quelles techniques de renseignement ont été utilisées à son sujet, mais l'autre partie le sait. De même, le requérant n'a pas accès à l'ensemble des pièces du dossier, alors que l'autre partie en a connaissance. IL en va également ainsi des arguments développés par l'administration, auxquels il n'est pas possible d'accéder.

Aussi bien, selon l'article L. 773-3 du code de justice administrative, l'intégralité des pièces produites par les parties est communiquée à la CNCTR mais pas au requérant lui-même. En outre, selon cette même disposition, les parties sont-elles entendu « *séparément lorsqu'est en cause le secret de la défense nationale* ».

La possibilité donnée au juge, en vertu de l'article L. 773-5 de ce code (« *La formation de jugement peut relever d'office tout moyen* ») n'est en rien suffisante pour pallier l'absence de contradictoire.

Au surplus, l'article L. 773-6 de ce même code ne permet pas au citoyen qui souhaite vérifier qu'il ne fait pas l'objet d'une surveillance d'en acquérir la certitude, étant donné que « *lorsque la formation de jugement constate l'absence d'illégalité dans la mise en œuvre d'une technique de recueil de renseignement ou du traitement faisant l'objet du litige,* […] *la décision indique au requérant ou à la juridiction de renvoi qu'aucune illégalité n'a été commise, sans confirmer ni infirmer la mise en œuvre d'une technique* ».

Cette procédure est donc manifestement contraire au droit au procès équitable protégé par l'article 16 de la Déclaration des droits, alors qu'il est constant que « *tant le principe de la séparation des pouvoirs que l'existence d'autres exigences constitutionnelles imposent [au législateur] d'assurer une conciliation qui ne soit pas déséquilibrée entre le droit des personnes intéressées à exercer un recours juridictionnel effectif, le droit à un procès équitable ainsi que la recherche des auteurs d'infractions et les exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation* » (Cons. const.,décision n° 2011-192 QPC, 10 novembre 2011, cons. 22).

Une telle conciliation n'existe pas en l'occurrence, puisque le principe du contradictoire disparaît sous les nécessités du renseignement. Cela est anormal en soi ; une telle négation l'est d'autant plus en l'occurrence que les motifs de la surveillance sont, on l'a vu, largement définis.