Monsieur le Président du Conseil Constitutionnel,

Mesdames et Messieurs les membres du Conseil,

2 rue Montpensier, 75002 Paris

***AMICUS CURIAE***

Monsieur le Président du Conseil Constitutionnel,

Vous avez été saisi de la loi relative au renseignement par Monsieur le Président de la République, Monsieur le Président du Sénat et plus de 60 députés, en application du deuxième alinéa de l'article 61 de la Constitution.

A l'aune de l'importance des questions soulevées par cette loi et des menaces qu'elle fait peser sur les libertés publiques, individuelles et personnelles, les associations professionnelles signataires de la présente opinion ont l'honneur de vous soumettre les observations suivantes sur les différents motifs d'inconstitutionnalité entachant ce texte. Nous appelons de nos vœux l'établissement d'un cadre juridique clair et protecteur des droits fondamentaux, qui permette que la lutte contre le terrorisme soit la plus efficace possible sans affecter la confiance et la transparence dans les outils et les usages numériques que promeuvent nos organisations, porteurs de progrès démocratique et social, de croissance et d'emplois pour notre pays.

**1.** Au préalable, afin d'éviter toute mauvaise compréhension de notre intervention, nous souhaitons rappeler notre attachement républicain à la poursuite de l'objectif constitutionnel de sauvegarde de l'ordre public et, particulièrement, de prévention des actes graves menaçant la sécurité des personnes. La lutte contre le terrorisme doit être sans concession et l'actualité nous le rappelle tragiquement. Elle appelle la mobilisation de toutes et tous, et les acteurs du secteur, quelle que soit leur taille, leur nationalité, leur métier, sont, à cet égard, prêts à prendre, et ont déjà pris, leurs responsabilités. Les entreprises de notre pays sont à l'unisson de la volonté

nationale de combattre les ennemis de la liberté sans faiblir mais sans renoncer à nos principes de droit

**Nous croyons qu'il est possible de renforcer les moyens de prévention des actes criminels les plus graves tout en préservant les équilibres indispensables pour la solidité d'une société démocratique, qui seuls permettront de préserver la confiance dans l'environnement numérique à laquelle nos associations professionnelles sont attachées. C'est pourquoi, nous considérons que les procédures dérogatoires au droit commun doivent être strictement et précisément définies, entourées de garanties réelles et effectives des droits et libertés fondamentaux, et proportionnées au but à atteindre**. **En l'occurrence, cet équilibre nous apparait rompu sur plusieurs aspects**. La volonté partagée par l'ensemble des citoyens français, comme par les autres peuples dans le monde, de combattre les actes de terreurs commis par les ennemis de la liberté, ne saurait servir d'alibi suffisant à la création d'un Etat d'urgence permanent. Ceci est d'autant plus vrai que la loi dont vous êtes saisi concerne, en réalité, bien d'autres menaces et enjeux que le terrorisme, mais affecte des pans entiers des activités de la société, sans que ni la vie des personnes ni même la sécurité des biens ne soient en danger.

Cet équilibre est au cœur de votre jurisprudence.

Le droit à la sécurité doit toujours être concilié avec le droit à la sûreté tel qu'il découle de l'article 2 de la Déclaration des Droits de l'Homme et du Citoyen de 1789, c'est-à-dire le droit à n'être ni surveillé, ni poursuivi, ni arrêté, arbitrairement. La liberté proclamée par ce même article implique le respect de la vie privée ainsi que vous l'avez jugé (Décisions n° 99-416 DC du 23 juillet 1999 ; n°2004-499 DC du 29 juillet 2004). De même, il est essentiel de s'assurer que la protection de la liberté personnelle soit pleine et entière au sens de l'article 16 de la Déclaration de 1789 disposant que « *Toute société dans laquelle la garantie des Droits n'est pas assurée, ni la séparation des pouvoirs déterminée, n'a point de Constitution* ».

D'autant plus que des actes de surveillance largement déployés et sans encadrement suffisant ou effectif peuvent affecter la présomption d'innocence protégée par l'article 9 et le principe de légalité des délits et des peines garantit au titre de l'article 7 de la Déclaration de 1789.

Il est essentiel que toute mesure de surveillance soit strictement proportionnée au but à atteindre et strictement encadrée.

Il est indispensable, en outre, que soit respecté le principe de clarté et d'intelligibilité de la loi fondé sur les articles 4, 6, et 16 de la Déclaration de 1789 tendant à protéger les citoyens de toute interprétation arbitraire d'une disposition législative par une autorité administrative ou judiciaire. Enfin, il ne peut faire de doute que le législateur doit épuiser sa compétence ainsi que l'exige l'article 34 de la Constitution dès lors que sont concernés les libertés. L'absence de précision ou le trop grand flou d'un texte législatif de cette nature est nécessairement dangereux et inconstitutionnel.

Dans votre rôle de gardiens des libertés, vous veillez toujours à ne pas substituer votre appréciation à celle souveraine du Parlement quant à l'opportunité des mesures attaquées. Pour autant, en matière de législation relative à la lutte contre le terrorisme, vous n'avez pas hésité à censurer une disposition pour disproportion manifeste au titre de la protection due à l'inviolabilité du domicile (Décision n° 96-377 DC du 16 juillet 1996, considérant 18).

**2.** Le numérique n'est pas à l'écart de ces principes et bénéficie tout pareillement de ces garanties. Vous-même, vous avez placé l'accès à l'Internet sous la protection de l'article 11 de la Déclaration de 1789 (10 juin 2009). L'accélération de l'utilisation des technologies du numérique ne doit donc pas signifier un affaiblissement des garanties pour nos droits. La garantie des libertés dans le monde physique est désormais étroitement liée à la protection des droits fondamentaux dans le monde dématérialisé.

C'est pourquoi, votre décision est attendue. Elle sera importante.

Elle s'inscrit dans un moment singulier de l'Histoire. Les révélations de Edward Snowden et celles encore récentes sur les pratiques de certains Etats démocratiques en matière de surveillance font que notre vie privée, nos données sont au cœur d'enjeux cruciaux pour nos sociétés. Il s'agit de protéger notre liberté personnelle et d'une certaine façon reconnaitre que beaucoup de notre vie et de nos actes sont hébergés dans un domicile virtuel en forme de prolongation indissoluble de notre domicile physique. La décision de la Cour Suprême des Etats-Unis Riley/Californie du 25 juin 2014 fondée sur le 4ème amendement de la Constitution américaine a montré l'importance des garanties judiciaires préalables lorsqu'il s'agit de la saisie par des autorités de police de données stockées dans un appareil numérique – un smartphone dans cette affaire. Cette décision rendue à l'unanimité est d'autant plus remarquable que son raisonnement, sous la plume du *Chief Justice* Roberts, montre à quel point les outils numériques, dont le *Cloud Computing* – l'informatique en nuage - expressément mentionné par la Cour (p. 21), contribuent à l'hébergement de notre vie privée. Ainsi, l'opinion de la Cour souligne-t-elle que la saisie des données stockées dans un smartphone ou dans le nuage peut révéler sur nous-mêmes et notre vie personnelle bien plus que la perquisition physique dans une maison (pages 20 à 23 de la décision) : notre localisation, nos déplacements, nos centres d'intérêts, nos opinions, nos relations, etc.

A maints égards, la protection de notre vie privée dans l'environnement numérique se rapproche de celle de notre domicile.

C'est dire que les questions qui vous sont posées engagent le futur de nos droits et libertés.

**3.** On le voit, **ce qui est en jeu ici tient bien à l'équilibre de notre Etat de droit. Aucun mécanisme de surveillance de masse n'est acceptable. De surcroît, lorsque sont adoptés des dispositifs de surveillance afin de prévenir certaines infractions, il est essentiel que les règles de leur encadrement soient d'une rigueur extrême afin de ne pas ouvrir la porte aux abus et détournements de pouvoir**.

Votre jurisprudence a dessiné un jardin à la française distinguant ce qui relève de la police judiciaire ou de la police administrative. Cette *summa divisio* vous conduit à accepter

qu'échappent au contrôle de l'Autorité Judiciaire prévue par l'article 66 de la Constitution pour garantir la liberté individuelle les activités relevant de la prévention des infractions (voir votre Décision du 19 janvier 2006, commentaire au Cahier n°20). L'article 66 renverrait, en effet, selon vous à l'*habeas corpus* c'est-à-dire au droit de ne pas être arbitrairement détenu. Qu'il nous soit permis de ne pas partager cette lecture dès lors que dans votre décision du 16 juillet 1996 rendue en matière de terrorisme (précitée) **vous aviez considéré que l'inviolabilité du domicile méritait la protection de l'autorité judiciaire au titre de la liberté individuelle**. Nulle détention n'était envisagée dans cette hypothèse…

Malgré les multiples demandes faites pendant les débats sur la loi en cause afin de placer les mesures de surveillance sous le contrôle du juge judiciaire, nous n'imaginons malheureusement pas, et nous le regrettons, que vous reveniez dans le cas présent sur cette distinction retenue dans votre décision de 2006.

En revanche, il est incontestable, et d'ailleurs pas vraiment contesté, que **la loi critiquée contribue à étendre spectaculairement le domaine de la police administrative. De fait, s'opère un glissement inquiétant, et de plus en plus large, de tout un pan des activités de surveillance qui sont alors exclues de la vigilance de l'Autorité judiciaire**. **Cette forme de déjudiciarisation intensive des investigations rend possible l'extension quasi indéfinie du domaine de la police administrative**. **Une telle évolution, dont cette loi est assez symptomatique, ne peut qu'inquiéter**. **Aussi, et dans ces conditions, elle oblige à ce qu'en conséquence le niveau des garanties attachées aux droits et libertés fondamentaux soit maintenu au plus haut voire, considérant les risques attachés à la puissance des procédés de la surveillance numérique, soit encore plus exigeant afin que toute disproportion manifeste entre le but poursuivi et les moyens mis en œuvre soit impossible. Il convient, en effet, d'éviter que l'Etat de droit ne se transforme sans crier gare en Etat de police**.

**Votre décision peut être fondatrice à maints égards d'un nouveau droit des libertés à l'ère numérique.**

**Elle doit être la réponse de la raison à la folie meurtrière des terroristes.**

* *

## ***SOMMAIRE***



* *

### I. <u>Sur l'article 2 de la loi quant au champ d'application des motifs justifiant le recours aux autorisations de surveillance</u>

Cet article définit le champ d'application des mesures d'interception des contenus, données et métadonnées. Il reprend largement certains des éléments initialement retenus par la loi du 10 juillet 1991 mais y ajoute des éléments élargissant très significativement le périmètre justifiant le recours aux procédés techniques d'interception et de surveillance.

On observera, <u>à titre liminaire</u>, qu'à notre connaissance **la loi du 10 juillet 1991 codifiée à droit constant par l'ordonnance du 12 mars 2012 n'a jamais fait l'objet d'un contrôle de conformité à notre Loi Fondamentale. Elle ne saurait donc bénéficier d'aucun brevet de constitutionnalité à cet instant**. Dès lors, et s'agissant des dispositions déjà existante mais modifiée par la présente loi, il pourra être fait application de votre jurisprudence dite « Nouvelle Calédonie » (DC du 25 janvier 1985) par laquelle vous avez jugé que « *la régularité au regard de la Constitution des termes d'une loi promulguée peut être utilement contestée à l'occasion de l'examen de dispositions législatives qui la modifient, la complètent ou affectent son domaine* ».

**I.1.** Force est d'admettre que le champ d'application résultant de l'article 1er de la présente loi méconnait le principe de légalité des délits et des peines et ensemble le principe de clarté et

d'intelligibilité de la loi fondé sur les articles 4, 6, et 16 de la Déclaration de 1789 tendant à protéger les citoyens de toute interprétation arbitraire par une autorité administrative ou judiciaire. Enfin, il ne peut faire de doute que l'article 34 de la Constitution est méconnu en raison du manque de précision de plusieurs éléments alors même que sont en cause les libertés fondamentales entachant dès lors la loi du vice d'incompétence négative.

C'est dans le même sens que la Cour Européenne des Droits de l'Homme a jugé que « *caractéristique de l'Etat policier, le pouvoir de surveiller en secret les citoyens n'est tolérable d'après la Convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques* » (CEDH, 6 septembre Klass/Allemagne, req. n°5029/71). Confirmant sa lecture de l'article 8 de la Convention, la même Cour dans son arrêt Uzun c/ Allemagne portant sur la surveillance par GPS (2010), a jugé qu' « *eu égard au risque d'abus inhérent à tout système de surveillance secrète, de telles mesures doivent se fonder sur une loi particulièrement précise, en particulier compte tenu de ce que la technologie disponible devient de plus en plus sophistiquée* ».

Pour mesurer, au cas présent, les manquements constitutionnels, il importe, encore une fois, d'établir un test de proportionnalité incluant l'amplitude des motifs retenus mise en regard des moyens immenses susceptibles d'être mis en œuvre pour surveiller les personnes. Autrement dit, le risque pour les droits de chaque personne sont d'autant plus importants que le motif justifiant la surveillance laisse la place à un trop grand pouvoir d'interprétation de l'autorité de police administrative pour déclencher les techniques de surveillance. On rappellera ici qu'en matière d'interception de sécurité, cela s'applique aussi à l'entourage des personnes concernée par l'autorisation (voir article L. 852-1 du Code de la Sécurité Intérieure - CSI).

**I.2.** Deux motifs sont particulièrement critiquables de ce point de vue.

En premier lieu, le motif de « *prévention de la criminalité et de la délinquance organisée* » encourt la même critique d'imprécision. Celui-ci repose sur la notion de « *bande organisée* » définie par l'article 131-7 du code pénal comme étant « *tout groupement formé ou toute entente en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions* ». La liste des infractions potentiellement concernées à ce titre est énoncée par l'article 706-73 du Code de procédure pénale qui fixe la liste des infractions, soit les cas suivants :

« *- 1° le crime de meurtre commis en bande organisée, passible de la réclusion criminelle à perpétuité en application de l'article 221-4 modifié du code pénal ;*

*- 2° le crime de tortures et d'actes de barbarie commis en bande organisée lorsqu'il est commis de manière habituelle sur un mineur de quinze ans ou sur une personne dont la particulière vulnérabilité, due à son âge, à une maladie, à une infirmité, à une déficience physique ou psychique ou à un état de grossesse, est apparente ou connue de son auteur, crime passible de trente ans de réclusion criminelle en application de l'article 222-4 modifié du code pénal ;*

*- 3° les crimes et délits de trafic de stupéfiants prévus par les articles 222-34 à 222-40 du code pénal, les peines encourues allant de cinq ans d'emprisonnement à la réclusion criminelle à perpétuité ;*

*- 4° les crimes et délits d'enlèvement et de séquestration commis en bande organisée, passibles de trente ans de réclusion criminelle ou de réclusion criminelle à perpétuité en application de l'article 224-5-2 nouveau du code pénal ;*

*- 5° les crimes et délits aggravés de traite des êtres humains sanctionnés par les articles 225-4-2 à 225-4-7 du code pénal, les peines encourues allant de dix ans d'emprisonnement à la réclusion criminelle à perpétuité ;*

*- 6° les crimes et délits aggravés de proxénétisme prévus par les articles 225-7 à 225-12 du code pénal, les peines encourues allant de dix ans d'emprisonnement à la réclusion criminelle à perpétuité ;*

*- 7° le crime de vol commis en bande organisée qui, en vertu de l'article 311-9 du code pénal, est passible de quinze à trente ans de réclusion criminelle ;*

*- 8° les crimes aggravés d'extorsion prévus par les articles 312-6 et 312-7 du code pénal, lorsque les violences ont entraîné une mutilation, une infirmité, la mort, des tortures ou actes de barbarie, ou lorsqu'elles ont été commises avec usage ou menace d'une arme, les peines encourues allant de vingt ans de réclusion criminelle à la réclusion criminelle à perpétuité ;*

*- 9° le crime de destruction, dégradation et détérioration d'un bien commis en bande organisée, lorsque celles-ci sont provoquées par une substance explosive, un incendie ou tout autre moyen de nature à créer un danger pour les personnes, la peine allant de vingt à trente ans de réclusion criminelle en vertu de l'article 322-8 modifié du code pénal ;*

*- 10° les crimes en matière de fausse monnaie prévus par les articles 442-1 et 442-2 modifiés du code pénal, passibles de dix ans d'emprisonnement à trente ans de réclusion criminelle ;*

*- 11° les crimes et délits constituant des actes de terrorisme prévus par les articles 421-1 à 421-5 modifiés du code pénal, la peine encourue allant jusqu'à la réclusion criminelle à perpétuité ;*

*- 12° les délits en matière d'armes commis en bande organisée prévus par des lois spéciales, passibles de dix ans d'emprisonnement en vertu des XVI à XXI de l'article 6 de la loi déférée ;*

*- 13° les délits d'aide à l'entrée, à la circulation et au séjour irréguliers d'un étranger en France commis en bande organisée prévus par le quatrième alinéa du I de l'article 21 de l'ordonnance du 2 novembre 1945 susvisée, puni par l'article 21 bis de la même ordonnance de dix ans d'emprisonnement ;*

*- 14° les délits de blanchiment prévus par les articles 324-1 et 324-2 du code pénal, ou de recel prévus par les articles 321-1 et 321-2 du code pénal, du produit, des revenus, des choses provenant des infractions mentionnées ci-dessus, passibles de cinq ou dix ans d'emprisonnement ;*

*- 15° les délits d'association de malfaiteurs ayant pour objet la préparation d'une des infractions mentionnées ci-dessus, punis par l'article 450-1 du code pénal de cinq ou dix ans d'emprisonnement ».*

Cette énumération que nous avons rappelée de façon exhaustive montre, d'une part, que **c'est tout un pan du droit pénal qui est ici concerné**. Parmi ces infractions, certaines sont d'une gravité extrême et visent, notamment, des **atteintes à la dignité humaine**. On y trouve aussi des **crimes et délits**, dont nonobstant la violation de l'ordre social, qui **ne sauraient être classés au rang de menaces pour l'intérêt national** et certainement pas justifier le recours à des procédés de surveillance massive. Un vol de tableau en bande organisée, le délit d'aide à l'entrée et au séjour des étrangers en situation irrégulière justifient-t-ils, par exemple, un tel régime de police administrative ? Non, à l'évidence non !

Ainsi que le relève la CNCDH dans son avis du 16 avril 2015, « *ces articles ne définissent pas un comportement incriminé, mais désignent un inventaire d'infractions dont le seul point commun est d'être commise en bande organisée sans que l'on sache exactement ce qu'est une bande organisée* » (§ 28).

En vertu de ce motif, c'est potentiellement une large partie du droit pénal qui serait ainsi partiellement dé-judiciarisé rendant dès lors possible la surveillance administrative tous azimuts, sans les procédures, attributs et contrôles de l'autorité judiciaire.

D'autre part, cette litanie d'infractions renvoie à des qualifications reposant sur des analyses et des qualifications préalables indispensables peu compatibles avec une surveillance massive dont on doit encore rappeler qu'elle peut s'étendre à l'entourage des personnes, au titre de la seule prévention des infractions, soit donc avant que l'infraction soit commise. Dans votre propre jurisprudence, on retrouve cette même préoccupation relative à la complexité de ces infractions. Ainsi, dans la décision de 2004 sur la loi portant adaptation de la justice aux évolutions de la criminalité, vous avez certes validé un mécanisme de procédure pénale, sous le contrôle de l'autorité judiciaire, reposant sur le renvoi aux articles 706-73 du CPP, mais vous l'avez assorti sur plusieurs points de réserves strictes d'interprétations.

« *Considérant que, parmi les infractions ne portant pas nécessairement atteinte aux personnes, figure le vol lorsqu'il est qualifié de crime ; que, toutefois, si le vol commis en bande organisée trouve sa place dans cette liste, il ne saurait en être ainsi que s'il présente des éléments de gravité suffisants pour justifier les mesures dérogatoires en matière de procédure pénale prévues à l'article 1er de la loi déférée ; que, dans le cas contraire, ces procédures spéciales imposeraient une rigueur non nécessaire au sens de l'article 9 de la Déclaration de 1789 ; qu'il appartiendra à l'autorité judiciaire d'apprécier l'existence de tels éléments de gravité dans le cadre de l'application de la loi déférée* » **et** *« qu'il ressort des termes mêmes de l'article 706-73 nouveau du code de procédure pénale que le délit d'aide au séjour irrégulier d'un étranger en France commis en bande organisée ne saurait concerner les organismes humanitaires d'aide aux étrangers ; que, de plus, s'applique à la qualification d'une telle infraction le principe énoncé à l'article 121-3 du même code, selon lequel il n'y a point de délit sans intention de le commettre* ».

Votre raisonnement illustre que la référence à ce motif affaiblit la frontière que vous avez patiemment dessinée pour distinguer la police administrative de la police judiciaire. Comme vous l'avez jugé, la plupart de ces infractions sont complexes et requiert un travail de qualification préalable qui ressort normalement de la compétence de l'autorité judiciaire. D'ailleurs, il est frappant de relever que s'agissant du délit d'aide à l'entrée et au séjour des étrangers en situation irrégulière, vous renvoyez à l'élément intentionnel. Or, par construction, cet élément ne peut être apprécié *in abstracto* avant la commission de l'infraction. **En décidant de surveiller tel groupe de personnes, ne fait-on pas de la justice prédictive, un pronostic sur l'avenir mais sans juge ?** A l'aune d'une telle liste d'infractions, il est difficile de prétendre qu'il s'agit seulement de prévention. Sans le dire expressément, la loi critiquée en reprenant ce motif tiré de la loi du 10 juillet 1991, remet en cause la cohérence de la distinction entre police administrative et police judiciaire et affaiblit les garanties liées aux droits et libertés fondamentaux dont bénéficie tout un chacun.

En second lieu, il convient de pointer le manque de clarté et le risque d'arbitraire lié à l'application du motif visant les « *violences collectives de nature à gravement porter atteinte à la paix publique* ». Là encore, nombreux sont ceux qui s'inquiètent qu'une telle définition ouvre sur une surveillance des mouvements syndicaux ou politiques.

Dans ces conditions, force est de constater que les motifs susvisés figurant dans l'article L. 811-3 nouveau du code de la sécurité intérieure sont entachés d'inconstitutionnalité.

## II. Sur l'article de la loi quant à l'absence d'autorisation préalable de la Commission Nationale de Contrôle des Techniques de Renseignement

**II.1.** La Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR) est consultée – sauf exception – *a priori* du recours aux techniques de surveillance. Cependant, cet **avis préalable ne lie pas le pouvoir exécutif et ne constitue aucunement une autorisation préalable. Ceci constitue une carence grave de la loi.**

Il s'évince, en effet, de votre propre jurisprudence, qu'en matière d'interception de données de connexion – et donc *a fortiori* si les contenus de communication sont concernés - l'autorisation préalable constitue l'une des garanties essentielles des exigences constitutionnelles.

Ceci résulte clairement notamment de votre décision n° 2005-532 DC du 19 janvier 2006 rendue sur saisine de sénateurs portant, déjà, sur une loi de prévention et de répression du terrorisme qui avait créé un dispositif d'interception des données de connexion, dans laquelle vous avez relevé que « *le I de l'article 6 de la loi déférée insère dans le code des postes et des communications électroniques un nouvel article L. 34-1-1 qui institue, " afin de prévenir et de réprimer les actes de terrorisme ", une procédure de réquisition administrative de données techniques de connexion ; que cette procédure sera mise en œuvre par des " agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions " ; qu'elle s'appliquera à toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public une connexion*

*permettant une communication en ligne par l'intermédiaire d'un accès au réseau ; qu'elle 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, la durée et la date des communications " **; qu'elle sera subordonnée à un accord préalable d'une personnalité désignée par la Commission nationale de contrôle des interceptions de sécurité** ;* »

En conséquence de quoi vous avez considéré *« qu'en l'espèce,* ***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*** ».

C'est ce que **confirme sans ambigüité** le commentaire autorisé fait aux Cahiers du Conseil Constitutionnel par le Secrétaire Général de l'institution (Cahiers n° 20) **qui relève à deux reprises que l'autorisation préalable prévue à l'article L. 34-1-1 du code des postes et communications électroniques constitue une garantie légale permettant de regarder comme constitutionnellement acceptable le mécanisme alors créé.**

**II.2.** Or, en l'occurrence, **le nouveau dispositif n'est pas soumis à une telle autorisation préalable**. Considérant le champ d'application du texte en cause, la durée des mesures de surveillance et la durée de conservation des données parfois sans limite précisée par la loi, le raisonnement que vous aviez suivi en 2006 doit s'appliquer de plus fort au cas présent. L'ensemble de la doctrine admet que la collecte de données et métadonnées - alors même qu'elles ne concerneraient pas le contenu des communications - permet aisément de tracer et reconstituer la vie privée des individus, y compris en cela de dresser leur profil personnel et donc leurs opinions politiques, philosophiques, religieuses, orientations sexuelles et toutes autres données sensibles ainsi que celles de leur entourage.

Considérant l'intensité de la surveillance rendue possible par la loi en cause, il est donc conforme à votre jurisprudence de 2006 que l'absence d'autorisation préalable entache d'un vice grave de constitutionnalité l'ensemble du mécanisme soumis à votre examen.

Il n'est pas indifférent de relever que nombreux sont les parlementaires et associations y compris de magistrats qui ont proposés pendant les débats parlementaires que l'avis de la CNCTR soit conforme.

L'avis de la CNCDH en date du 16 avril 2015 va clairement dans ce sens en soulignant que *« Seul un avis préalable et conforme constituerait une véritable garantie* » (§ 39 et 40).

C'est en vain qu'il serait opposé que la loi du 10 juillet 1991 se contentait, pour sa part, de prévoir un avis simple de la CNCIS sur les décisions prises par le Premier Ministre. D'abord,

cette loi n'ayant jamais été déférée à votre examen, il ne peut être sérieusement considéré qu'elle aurait été *a priori* conforme à la Constitution, sur ce point tout du moins.

Ensuite, et comme il a déjà été dit, la présente loi étend de façon radicale tant les motifs de surveillance que les autorités susceptibles d'y recourir et les techniques utilisables. **Nul ne comprendrait qu'une extension, inédite dans notre histoire, des capacités de surveillance des individus, se traduise par une diminution corollaire des protections légales dues à toute personne. Au contraire, c'est le raisonnement inverse qui est constitutionnellement le plus fondé : l'accroissement des pouvoirs de police administrative en matière de surveillance et donc d'intrusion dans la vie privée requiert un niveau plus intense de garantie des droits.** De surcroît, les garanties constitutionnelles ne sauraient être regardées comme amoindrissant par nature l'efficacité préventive espérée des mécanismes de surveillance administrative en question.

C'est donc bien à l'aune de votre jurisprudence de 2006 qu'il faut apprécier le présent dispositif, lequel s'avère manifestement entaché d'une absence de garanties suffisantes au regard des exigences constitutionnelles.

Dès lors que le régime des avis de la CNCTR est un élément substantiel du dispositif, nul doute que le caractère inséparable de ces dispositions du reste du texte aboutira à une censure de l'ensemble du mécanisme. Une telle invalidation totale ne serait cependant pas un obstacle majeur à la mise en œuvre des mesures de prévention du terrorisme puisque Monsieur le Président de la République pourra demander une seconde délibération en vertu de l'alinéa second de l'article 10 de la Constitution, afin que le législateur complète la loi en indiquant que l'avis de la CNCTR est conforme et donc constitue une autorisation préalable.

La censure du tout interviendra en conséquence.

**II.3.** C'est en vain qu'il serait soutenu que doter la CNCTR d'un pouvoir d'autorisation préalable aurait porté atteinte au principe de la séparation des pouvoirs.

Il a été certes dit lors des débats devant le Parlement qu'une autorité administrative ne pouvait pas empiéter sur le domaine régalien dévolu au Premier ministre car il en irait de la séparation des pouvoirs.

Cette argumentation ne résiste pas à l'analyse.

**Notre Constitution permet tout à fait à une autorité administrative indépendante de prendre des décisions contraignantes dans des domaines circonscrits, sans méconnaitre le principe de séparation des pouvoirs**. C'est vrai tant dans les rapports avec l'autorité judiciaire qu'avec l'autorité administrative (Décision du 17 janvier 1989 DC n°88-248 DC, considérant 27). **D'ailleurs, dans votre décision de 2006, l'avis préalable donné par une personne désignée par la CNCIS n'a pas été regardé comme méconnaissant la répartition des compétences institutionnelles**.

La CNCTR a, selon la loi critiquée, le statut d'autorité administrative indépendante. Pour reprendre ici l'expression du Professeur J. Chevallier, cette « diffraction du pouvoir étatique » ne fait pas obstacle à la séparation des pouvoirs et ce d'autant moins que cette autorité a pour objet

même de garantir des droits et libertés fondamentaux constitutionnellement protégés. En la dotant d'un pouvoir d'autorisation préalable, le législateur n'aurait pas commis un empiètement sur les compétences du Premier Ministre telles qu'elles ressortent de l'article 21 de la Constitution, mais, au contraire, aurait permis la mise en œuvre de techniques de surveillance aux fins de prévention d'un certain nombre d'infractions potentielles entourées par des garanties constitutionnelles adaptées aux menaces pour les libertés.

On doit même considérer que le statut d'autorité administrative indépendante dont la CNCTR a été dotée ruine, par construction, l'argutie tiré d'une prétendue atteinte au principe de la séparation des pouvoirs.

**Il existe, d'ailleurs, des exemples où une autorité administrative indépendante exerce un tel pouvoir vis-à-vis des prérogatives du gouvernement. Ainsi, entre 1978 à 2004, l'article 31 de la loi n°78-17 « Informatique & Libertés » a doté la CNIL d'un pouvoir d'autorisation *« par avis conforme »* des fichiers de police administrative intéressant la sûreté de l'Etat, la défense ou la sécurité publique**.

Les DST, DGSE et Renseignements Généraux de cette époque ont pu, par l'ensemble des décrets adoptés sur avis conformes de la CNIL et du Conseil d'Etat dès le début des années 80, mettre en œuvre des traitements de données personnelles relatifs à leurs missions dans ces domaines. La CNIL était également dotée par la loi n° 78-17 d'un pouvoir de contrôle *a posteriori* inopiné des fichiers constitués par ces administrations dotées de pouvoirs régaliens et pouvait prendre à leur égard des décisions contraignantes à caractère juridictionnel, susceptibles de recours par les administrations concernées devant le Conseil d'Etat.

De tous ces chefs, la censure est inévitable.

## III. Sur les conditions de renouvellement des autorisations délivrées par le Premier Ministre pour les opérations de surveillance

**III.1.** Les autorisations délivrées par le Premier Ministre sont susceptibles d'être renouvelées dans les mêmes conditions que l'autorisation initiale. Il est cependant frappant de constater que la loi ne prévoit aucune limite effective dans le temps pour ces renouvellements d'autorisation.

Les durées prévues par la loi pour les différentes autorisations sont :

| Articles du code de la sécurité intérieure | Durée initiale d'autorisation | Conditions de renouvellement | Nombre de renouvellements possibles |
|---|---|---|---|
| Art. L. 821-4 | Quatre mois | Renouvelable dans les mêmes conditions de durée que l'autorisation initiale | Sans limite précisée par la loi |
| Art. L. 851-3 | Deux mois | | |
| Art. L. 851-4 | Deux mois | Quatre mois | |
| Art. L. 851-7 | Deux mois | Renouvelable dans les mêmes conditions de durée que l'autorisation initiale | |
| Art. L. 852-1 | 48H | « renouvelable » | |
| Art. L. 853-1 | Deux mois | Renouvelable dans les mêmes conditions de durée que l'autorisation initiale | |
| Art. L. 853-2 | 30 jours ou 2 mois | | |
| Art. L. 853-3 | 30 jours | | |
| Art. L. 854-1 | 4 mois | « renouvelable » | |

Les durées initiales d'autorisation ainsi que l'absence de limite dans le temps des renouvellements possibles doivent être mises en perspective, une nouvelle fois, avec l'extension des moyens de surveillance des individus et de leur entourage, y compris lorsqu'il s'agit de communications internationales. Ce dispositif est donc insuffisamment encadré dans le temps et partant, méconnait l'exercice des libertés constitutionnellement garanties au nombre desquelles 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.

Vous avez déjà eu l'occasion de statuer sur un dispositif similaire, certes validé mais en raison précisément des garanties procédurales prévues par la loi. Saisi d'un dispositif autorisant à l'initiative du procureur de la République l'enregistrement et la transcription de correspondances émises par la voie des télécommunications, vous avez jugé, dans votre décision n° 2004-492 DC du 2 mars 2004, « *que cette autorisation est délivrée pour une durée maximale de quinze jours, **qui n'est renouvelable qu'une fois**, sous le contrôle du juge des libertés et de la détention* » et « *que, **dans ces conditions**, les dispositions critiquées ne portent une atteinte excessive ni au secret de la vie privée ni à aucun autre principe constitutionnel* » (considérants 59 et 61).

Ainsi donc le fait que **l'autorisation limitée dans le temps à 15 jours une fois renouvelable** constitue l'une des conditions de validité du dispositif montre amplement qu'une autorisation de ce type doit être nécessairement bornée dans l'espace et le temps, sauf à créer une atteinte disproportionnée à la vie privée et à la liberté des individus.

Certes, dans le cas de 2004, il s'agissait des conditions de mise en œuvre d'un procédé de surveillance dans le cadre d'une opération de police judiciaire, c'est-à-dire placée donc sous le contrôle du juge judiciaire. Il demeure que le raisonnement que vous avez alors suivi peut parfaitement s'appliquer au cas présent. On est même tenté d'écrire *a fortiori*. La circonstance que les dispositifs en cause soient liés à des activités de police administrative ne saurait exonérer le législateur de la nécessité de fixer des limites temporelles à la durée des autorisations de surveillance, y compris leur renouvellement potentiel.

On éprouverait même quelque difficulté à comprendre pourquoi le contrôle du juge judiciaire devrait être plus strictement encadré quand il s'inscrit dans la logique de l'article 66 de la Constitution, alors que l'exercice du pouvoir de police administrative échapperait à cette garantie constitutionnelle. **Il ne serait pas sérieux de soutenir que la différence tient au fait que la liberté individuelle touche à la seule détention des personnes. En effet, votre décision de 2004 ne concerne pas une décision de privation de liberté, mais bien les conditions de mise en œuvre de techniques de surveillance menaçant la vie privée**.

**III.2.** Or, en l'espèce, la loi prévoit que chaque autorisation est « *renouvelable dans les mêmes conditions* » que l'autorisation initiale. **Ainsi rédigé, le dispositif ne cantonne pas le renouvellement à une seule fois, mais peut très bien aboutir à une succession indéfinie d'autorisations rendant le dispositif de surveillance illimité dans le temps, ou à tout le moins se répétant sur une période excessivement longue au regard des droits et libertés fondamentaux susceptibles d'être affectés**. Il est essentiel de garder à l'esprit que cette question de durée doit être mise en perspective avec le large champ d'application de la loi, les techniques de surveillance utilisables et le nombre de personnes susceptibles d'être concernées dont, dans certaines circonstances, leur entourage -personnel ou professionnel.

Considérant l'ampleur des actes de surveillance ainsi envisageables, il est certain que cette absence de limite dans le temps constitue une atteinte gravement disproportionnée à la liberté personnelle et à la vie privée. Rien, à cet égard, ne pourrait justifier que les procédés sous le contrôle du juge judiciaire soient plus strictement encadrés, comme vous l'avez admis en 2004, quand les dispositifs de police administrative ne connaitraient, pour leur part, aucune limite temporelle établie par la loi, ni ne seraient susceptibles de faire l'objet d'une autorisation préalable, fut-elle administrative.

A supposer, pour les seuls besoins du raisonnement, que vous ne jugiez pas en tant que telles ces amplitudes de surveillance des individus comme contraires à l'article 2 de la Déclaration de 1789, il resterait que le législateur, en ne précisant pas combien de fois ce renouvellement peut intervenir est demeuré en deçà de sa propre compétence telle que définie par l'article 34 de la Constitution.

Il eût fallu, à tout le moins, que le législateur précisât que le renouvellement ne pourrait se faire qu'une seule fois dans les mêmes conditions, et voyant mal comment une simple réserve d'interprétation pourrait pallier cette carence du législateur, la censure est donc inévitable.

## IV. <u>Sur l'article 2 de la loi et les durées de conservation des données et métadonnées recueillies dans le cadre des opérations de surveillance prévues par la loi</u>

**IV.1.** La loi attaquée prévoit différentes durées de conservation des données collectées au titre des opérations de surveillance autorisées par le Premier Ministre :

| | |
|---|---|
| Art. L. 822-2 du code de la sécurité intérieure | 1° 30 jours à compter de leur recueil<br>2° 120 jours à compter de leur recueil |

| | |
|---|---|
| | 3° 4 ans à compter de leur recueil<br>Et 6 ans à compter de leur recueil pour les donnée chiffrées<br>*NB : peuvent être conservés au-delà de ce délai 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.* |

Certaines de ces données ainsi collectées et placées dans des fichiers sont relatives au contenu de conversations ou d'échanges écrits, quand d'autres sont dites « métadonnées ». L'impact sur la vie privée est particulièrement évident s'agissant du contenu même des communications. Il l'est tout autant, sinon plus, s'agissant de ces métadonnées. La notion de "métadonnée" n'est pas nouvelle puisque celle-ci a émergé au sein de nos sociétés dans les années 60. La métadonnée est en règle générale qualifiée de "*donnée sur une autre donnée*" ou d'"*information sur une autre information*": il s'agit "*d'un niveau caché d'information additionnelle automatiquement créée et incorporée dans un fichier informatique*". Si l'on prend, par exemple, un courriel, on dira que la donnée est le contenu du courriel alors que ses métadonnées sont les informations qui caractérisent le courriel, c'est-à-dire l'heure, la date, le lieu de l'envoi, l'expéditeur, le destinataire, l'objet du courriel, les étapes techniques et infrastructures informatiques intervenues durant son transport, l'identification du terminal de l'expéditeur et du destinataire, le système d'exploitation de chaque terminal, etc. En ce qui concerne une photographie ou une vidéo, les métadonnées permettent de révéler l'heure ainsi que la date et le lieu où celle-ci a été prise, de même que sa taille, son poids et le format du fichier, le modèle de matériel utilisé pour la prise de vue, le numéro de série ou l'identifiant unique de ce matériel, etc.

Toutefois, les métadonnées d'un courriel ou autre peuvent dévoiler énormément d'informations susceptibles de porter atteinte à la vie privée et aux données personnelles d'un individu. En effet, dans le cas d'un courriel par exemple, la simple lecture des métadonnées des emails d'un individu permettent d'établir sa localisation, notamment le lieu de son domicile, de ses rendez-vous, de son travail, ses relations, ou encore, dans certains cas, ses opinions politiques, philosophiques, religieuses, ses problèmes de santé, etc.

Il est certain que ces informations sont protégées au titre de la vie privée que vous garantissez en application de l'article 2 de la Déclaration de 1789, sauf à considérer qu'une donnée informatique imputable à une personne physique identifiable, même indirectement, ne constituerait pas une donnée à caractère personnel relevant de la vie privée. Or, il ne pourrait être sérieusement soutenu, par exemple, que la loi n° 78-17 « Informatique & Libertés » ne s'appliquerait qu'au traitement de l'identification directe des personnes physiques et non aux traces et métadonnées que leur usage de l'informatique révèle d'elles-mêmes et de leurs comportements. Une telle thèse serait non seulement contraire à la décision 2004-499 DC rendue par le Conseil constitutionnel le 29 juillet 2004, mais elle conduirait aussi à conclure que les métadonnées n'auraient aucun intérêt pour les activités de renseignement, alors qu'elles sont logiquement au cœur des activités de surveillance.

**IV.2.** On en voudra pour confirmation, la décision de la Cour de Justice de l'Union Européenne confirmée par la Cour Constitutionnelle de Belgique.

Les métadonnées étaient, en effet, dans le champ de la Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 *sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE* annulée par la Cour de Justice de l'Union européenne dans un arrêt *Digital Right Ireland Ltd.* du 8 avril 2014.

Cette Directive prévoyait de pouvoir "*tracer et identifier la source de communication", "identifier la date, l'heure et la durée d'une communication", "identifier le type de communication", "identifier la machine utilisée pour communiquer", "identifier la location des équipements de communication"*. La Cour de Justice de l'Union européenne a considéré que « ***ces données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes (…) telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci*** ». Pour la Cour, ce texte portait une atteinte disproportionnée aux articles 7 et 8 de la Charte des droits fondamentaux relatifs respectivement au *"Respect de la vie privée et familiale"* et à la "*Protection des données à caractère personnel*". La Cour a notamment relevé que le fait que la conservation illimitée de données personnelles d'individus par les autorités nationales méconnaissait ces droits dans la mesure où : "*l'obligation de conservation couvre de manière généralisée toute personne, tous les moyens de communication électronique et l'ensemble des données relatives au trafic, sans différenciation, limitation ou exception opérées en fonction de l'objectif de lutte contre les infractions graves", "l'accès ouvert aux données collectées est trop large et est encadré de manière insuffisante", "cet accès ne fait pas l'objet d'un contrôle préalable par une juridiction ou une autorités indépendante", "aucune durée de conservation précise n'est imposée aux États, seule une fourchette de 6 mois à 2 ans étant prévue, sans distinction entre les personnes, ni les infractions concernées"*. Très récemment, la Cour Constitutionnelle de Belgique par un arrêt du 11 juin 2015 (n°84-2015) a censuré la loi nationale de transposition en faisant une application rigoureuse de cette décision de la Cour Européenne.

C’est dire que la collecte et la conservation des données et métadonnées doivent être strictement limitées dans leur champ et leur durée.

**IV.3.** Au cas présent, il est certain que les durées énumérées ci-dessus sont d’une durée trop longue au regard de l’objectif de la loi et ne sont assorties d’aucun contrôle effectif au sens de la loi n° 78-17, puisque la CNCTR ne dispose d’aucun pouvoir impératif de contrôle en la matière.

Force est de constater que ces durées varient de quelques jours à plusieurs années. Certes, dans certains des cas prévus, les longues durées correspondent à des besoins d’enquêtes les plus complexes, relatives aux infractions les plus graves. Il demeure que, par exemple, la conservation possible pendant 6 ans des renseignements chiffrés à compter de leur recueil apparait singulièrement extensive et manifestement disproportionnée, puisque la mise au clair de ces données durant cette période de six années n’entraîne aucune autre durée de conservation qui serait calquée sur celle applicable à des données initialement recueillies en clair. Pareillement, il est prévu au dernier § du I de l’article L. 822-2 du CSI que peuvent être conservés au-delà de ces délais 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. Dans ce cas, aucune limite de temps n’est fixée par la loi. Si l’on comprend bien la nature singulière des situations concernées par cette disposition, il reste qu’il est constitutionnellement délicat de ne pas prévoir une période raisonnable de conservation précisément définie, serait-elle plus longue que la moyenne eu égard aux circonstances particulières qu’il s’agit d’appréhender.

De même, s’agissant des informations et documents mentionnés à l’article L. 851-1 nouveau du CSI, nul doute que la durée de conservation de 4 ans est trop longue dès lors que leur recueil intervient dans le cadre d’une procédure de police administrative, donc de prévention d’infractions par nature non commises.

**Enfin, rien n’est prévu s’agissant du contrôle des fichiers constitués ou nourris par les données et métadonnées collectées au titre des opérations de surveillance réalisées au titre de la présente loi.**

D’une part, la CNCTR ne dispose d’aucun pouvoir impératif de décision en la matière. D’autre part, les données et métadonnées qui auraient été analysées par les services de renseignement comme étant non nécessaires au regard des finalités fixées par la loi, ne font l’objet d’aucune obligation de destruction à bref délai, ni même d’aucun pouvoir pour la CNCTR ni pour le Conseil d’Etat d’en ordonner la purge.

Sur ce point, le législateur a non seulement écarté tout contrôle de la conservation des données et métadonnées utiles aux activités de renseignement, mais il a également organisé la conservation de données et métadonnées qui seraient pourtant été analysées par les administrations concernées, comme étant parfaitement inutiles aux activités de renseignement.

La censure est ici également encourue.

## V. Sur l'article 2 et les recours relatifs à la mise en œuvre des techniques de renseignement soumises à « autorisation » et des fichiers intéressants la sûreté de l'Etat

L'article 2 de la loi crée un Titre IV dans le code de sécurité intérieure organisant les voies de recours relatifs à la mise en œuvre des techniques de renseignement organisées par ailleurs. Le juge compétent est le Conseil d'Etat. Il ne sera pas discuté cette attribution de compétence dès lors que d'une part, vous considérez que les mesures de surveillance aux fins de prévention des infractions relèvent de la police administrative et donc du juge administratif et que, d'autre part, le Conseil d'Etat est fondamentalement attaché à la protection des droits et libertés fondamentaux.

Nonobstant cette logique, il apparait que le droit au recours tel que garantit par l'article 16 de la Déclaration de 1789 est méconnu pour au moins deux motifs.

**V.1.** D'une part, la loi a certes prévu une voie de recours ouverte à toute personne, mais les conditions de son accès sont pour le moins contraire à la logique du droit au recours. D'abord, la personne doit saisir au préalable la CNCTR. Mais l'article L. 833-4 nouveau du CSI organisant cette saisine ne prévoit aucun délai de réponse de la Commission au requérant. De plus, la réponse prévue n'indique pas si oui ou non une technique de renseignement a été mise en œuvre le concernant. La CNCTR doit se borner à indiquer qu'elle a procédé aux vérifications, mais il lui est interdit de préciser au requérant ce qu'il en faut en inférer. On se demande bien à quoi sert du point du vue de l'exercice du droit de recours une procédure préalable obligatoire dont l'enjeu est de n'avoir pas de réponse à la question posée…

Ensuite de quoi, si l'intéressé persiste, il peut saisir le Conseil d'Etat qui statue selon une procédure particulière et partiellement secrète. Ce qui est gênant d'un point de vue constitutionnel, c'est que le code de justice administrative (CJA) est modifié et limite les conséquences du constat d'une illégalité constatée au titre de cette procédure. Ainsi, en effet, le nouvel article L. 773-7 du CJA prévoit que le Conseil d'Etat, s'il constate qu'une technique de recueil de renseignement a été mise en œuvre illégalement ou qu'un renseignement a été conservé illégalement, **peut** annuler l'autorisation et ordonner la destruction des renseignements irrégulièrement collectés.

Autrement dit, l'illégalité d'une autorisation n'entraîne pas nécessairement son annulation.

.

On ajoutera que dans l'hypothèse de la mise en œuvre d'une technique de recueil de renseignements au titre de l'article L. 851-3 nouveau du CSI, il sera bien délicat de savoir qui a été surveillé ou non dès lors que cela peut porter sur plusieurs centaines voire milliers de personnes… Sans doute aurait-il été pertinent d'imaginer que soit institué une action de groupe ouverte dans des conditions très limitées à des associations de défense des droits et libertés afin de saisir le Conseil d'Etat de recours d'intérêt général. A tout le moins, le législateur aurait-il dû prévoir un cas d'intervention spécifique pour ce type d'association.

Non seulement, une action de cette nature est délicate à engager pour un particulier mais, de surcroit, elle peut s'avérer lourde à gérer sur la longueur.

Il en résulte que la procédure prévue par la loi est insuffisante au regard des menaces pour les libertés. Ceci est manifestement contraire au droit au recours et à un procès équitable et rend, *de facto*, impossible pour un individu la protection de ses libertés.

**V.2.** D'autre part, la loi ne prévoit aucune voie de recours ouverte aux opérateurs et autres personnes morales exploitant un réseau à qui les autorités compétentes demanderaient d'agir d'une façon ou d'une autre au titre des techniques de recueil de renseignement et particulièrement lorsqu'il s'agit de placer une sonde sur un réseau exploité par eux.

Or, un opérateur peut être placé dans la situation de considérer que telle ou telle demande n'est pas conforme à la loi et s'opposer à une demande faite sur le fondement du code de la sécurité intérieure et par exemple refuser la pose d'une sonde sur son réseau. Cette hypothèse peut paraitre d'école. Il reste qu'elle peut parfaitement devenir une réalité si, dans le futur, les autorités compétentes avaient une gestion inappropriée des textes.

**Ce risque est d'autant moins hypothétique que l'article 5 de la loi autorisant les techniques de surveillance du réseau crée de nouveaux articles dans le code de la sécurité intérieure, dont le champ d'application est flou et imprécis** (**voir VI. ci-après**). C'est dire que les opérateurs risquent de se retrouver confrontés à des demandes juridiquement contestables sans pouvoir s'y opposer sur le plan contentieux, sauf à concevoir que le droit commun s'applique alors. Cette dernière hypothèse ne ressortant pas évidemment du silence absolu du texte à cet égard, il est, dans ces conditions, difficile de pallier une telle carence par une simple réserve qui aboutirait à réécrire l'article.

La question est d'autant moins secondaire que l'intensité maximale d'intrusion dans les réseaux que permet le texte ne peut que conduire à porter atteinte, en outre, à la liberté d'entreprendre. Cela ne peut que saper la confiance dans l'économie numérique.

L'invalidation de l'article est inévitable. **Ce dispositif relatif au droit au recours étant, en effet, indispensable à l'équilibre du texte et partant au respect de la Constitution, s'avère inséparable de l'ensemble. Cette annulation inévitable aboutira à une censure totale conduisant là encore à une seconde délibération en application de l'article 10 de la Constitution**.

## VI. Sur l'article 5 de la loi et la mise en œuvre de procédés de surveillance algorithmique

**VI.1.** L'article 5 de la loi prévoit dans aux articles L. 851-3 et L. 851-4 nouveaux du Code de la Sécurité Intérieure un dispositif de recueil en temps réel sur les réseaux des opérateurs et des personnes mentionnées à l'article L. 851-1 du même code - incluant donc les personnes visées par l'article L. 34-1 du Code des Postes et Communications Electroniques (CPCE), qui vise *« toutes informations et documents »*, 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.

Sont ainsi directement visées des métadonnées telles que définies précédemment, soit donc des informations protégées au titre de l'article 2 de la Déclaration de 1789 garantissant la vie privée et la liberté personnelle. Dès lors, il est essentiel que la loi soit à cet égard suffisamment claire et précise.

Or, il est patent que les articles ici critiqués méconnaissent le principe de clarté et d'intelligibilité de la loi fondé sur les articles 4, 6, et 16 de la Déclaration de 1789 tendant à protéger les citoyens de toute interprétation arbitraire par une autorité administrative ou judiciaire et ensemble, l'article 34 de la Constitution entachant d'incompétence négative le dispositif.

**VI.2.** En premier lieu, le texte en cause manque à cet égard des précisions indispensables dès lors, en effet, que la notion de « réseau » n'est absolument pas définie par la loi critiquée.

En particulier, reste totalement ouverte la question de savoir où seront placées les sondes algorithmiques sur les réseaux de communications électroniques - qui peuvent être tant publics que privés. Cette question touche plus largement l'absence de définition juridique dans les articles concernés de la notion de « réseau » applicable en l'espèce. Certes, il est loisible de s'en remettre aux définitions de l'article L.32 du CPCE dont on doit avouer qu'elle couvre un champ d'hypothèses extrêmement larges :

*« 2° Réseau de communications électroniques.*

*On entend par réseau de communications électroniques toute installation ou tout ensemble d'installations de transport ou de diffusion ainsi que, le cas échéant, les autres moyens assurant l'acheminement de communications électroniques, notamment ceux de commutation et de routage.*

*Sont notamment considérés comme des réseaux de communications électroniques : les réseaux satellitaires, les réseaux terrestres, les systèmes utilisant le réseau électrique pour autant qu'ils servent à l'acheminement de communications électroniques et les réseaux assurant la diffusion ou utilisés pour la distribution de services de communication audiovisuelle.*

*3° Réseau ouvert au public.*

*On entend par réseau ouvert au public tout réseau de communications électroniques établi ou utilisé pour la fourniture au public de services de communications électroniques ou de services de communication au public par voie électronique.*

*3° bis Points de terminaison d'un réseau.*

*On entend par points de terminaison d'un réseau les points physiques par lesquels les utilisateurs accèdent à un réseau de communications électroniques ouvert au public. Ces points de raccordement font partie du réseau.*

*3° ter Boucle locale.*

*On entend par boucle locale l'installation qui relie le point de terminaison du réseau dans les locaux de l'abonné au répartiteur principal ou à toute autre installation équivalente d'un réseau de communications électroniques fixe ouvert au public.*

*4° Réseau indépendant.*

*On entend par réseau indépendant un réseau de communications électroniques réservé à l'usage d'une ou plusieurs personnes constituant un groupe fermé d'utilisateurs, en vue d'échanger des communications internes au sein de ce groupe.*

*5° Réseau interne.*

*On entend par réseau interne un réseau de communications électroniques entièrement établi sur une même propriété, sans emprunter ni le domaine public-y compris hertzien-ni une propriété tierce.*

*(...)*

*9° Interconnexion.*

*On entend par interconnexion la liaison physique et logique des réseaux ouverts au public exploités par le même opérateur ou un opérateur différent, afin de permettre aux utilisateurs d'un opérateur de communiquer avec les utilisateurs du même opérateur ou d'un autre, ou bien d'accéder aux services fournis par un autre opérateur. Les services peuvent être fournis par les parties concernées ou par d'autres parties qui ont accès au réseau. L'interconnexion constitue un type particulier d'accès mis en œuvre entre opérateurs de réseaux ouverts au public.*

*10° Equipement terminal.*

*On entend par équipement terminal tout équipement destiné à être connecté directement ou indirectement à un point de terminaison d'un réseau en vue de la transmission, du traitement ou de la réception d'informations. Ne sont pas visés les équipements permettant exclusivement d'accéder à des services de radio et de télévision.*

*11° Réseau, installation ou équipement radioélectrique.*

*Un réseau, une installation ou un équipement sont qualifiés de radioélectriques lorsqu'ils utilisent des fréquences radioélectriques pour la propagation des ondes en espace libre. Au nombre des réseaux radioélectriques figurent notamment les réseaux utilisant les capacités de satellites ;*

*(...)*

*17° Itinérance locale.*

*On entend par prestation d'itinérance locale celle qui est fournie par un opérateur de radiocommunications mobiles à un autre opérateur de radiocommunications mobiles en vue de permettre, sur une zone qui n'est couverte, à l'origine, par aucun opérateur de radiocommunications mobiles de deuxième génération, l'accueil, sur le réseau du premier, des clients du second.*

*17° bis Itinérance ultramarine.*

*On entend par prestation d'itinérance ultramarine celle qui est fournie par un opérateur de radiocommunications mobiles déclaré sur le territoire de la France métropolitaine, d'un département d'outre-mer, de Mayotte, de Saint-Barthélemy, de Saint-Martin ou de Saint-Pierre-et-Miquelon à un autre opérateur de radiocommunications mobiles fournissant des services de communications mobiles sur réseau public terrestre dans un autre de ces territoires, en vue de permettre l'utilisation du réseau du premier, dit " opérateur du réseau visité ", par les clients du second, dit " opérateur du réseau d'origine ", pour émettre ou recevoir des communications à destination de l'un de ces territoires ou d'un Etat membre de l'Union européenne.*

*(...)*

*19° Ressources associées.*

*On entend par ressources associées les infrastructures physiques et les autres ressources associées à un réseau de communications électroniques ou à un service de communications électroniques, qui concourent ou peuvent concourir à la fourniture de services via ce réseau ou ce service. Sont notamment considérés comme des ressources associées les bâtiments ou accès aux bâtiments, le câblage des bâtiments, les antennes, tours et autres constructions de soutènement, les gaines, conduites, pylônes, trous de visite et boîtiers.*

*20° Services associés.*

*On entend par services associés les services associés à un réseau ou à un service de communications électroniques et qui concourent ou peuvent concourir à la fourniture de services via ce réseau ou ce service. Sont notamment considérés comme des services associés les services de conversion du numéro d'appel, les systèmes d'accès conditionnel, les guides électroniques de programmes, ainsi que les services relatifs à l'identification, à la localisation et à la disponibilité de l'utilisateur. »*

On le voit, le CPCE comporte de nombreuses « sous-définitions » telles que celle de « réseau public », « réseau interne » et on ne sait si ces distinctions seront retenues pour application des articles L. 851-3 et L. 851-4 et notamment la possibilité de surveiller des « réseaux indépendants » correspondant à un « groupe fermé d'utilisateurs »…).

Pour le placement de ces sondes algorithmiques, il existe, de fait, deux grandes possibilités qui permettent en réalité de couvrir quasiment tous les points des réseaux :

(i) Soit en extrémité de réseau, ce qui suppose d'intervenir sur plusieurs dizaines de milliers d'équipements (plus particulièrement cela ouvre une large possibilité pour les services du renseignement de toucher les équipements des hébergeurs (même si ces équipements ne sont pas détenus en propre par ces acteurs, la loi ne faisant aucune référence aux « réseaux » propriétaires ou aux équipements de réseaux propriétaires), au-delà des opérateurs de communication électroniques. En ce sens, les équipements concernés sont incommensurables : les câbles sous-marins, les points de présence, les capacités en fibre, etc.

(ii) Soit sur les cœurs de réseau ou sur les routeurs d'interconnexion. Si tel était le cas, cela nécessiterait de recourir à un équipement supplémentaire afin de recueillir d'autres métadonnées que les données de connexion, en mettant en place des équipements en cœur de réseau, des « *deep packet inspection* ». Ces équipements sont extrêmement intrusifs, puisqu'ils analysent l'ensemble des données qui circulent sur un réseau de communications électroniques. Ils seront clairement caractéristiques d'une surveillance de masse, résolument étrangère à toute notion de finalité et de proportionnalité.

Interrogé sur ce point par les députés Laure de la Raudière et Lionel Tardy, Monsieur le Ministre Jean-Yves Le Drian, a répondu que « ***La méthode de mise en œuvre des traitements sera en outre négociée avec les opérateurs ou les prestataires concernés en fonction des situations et des besoins*** »(Assemblée Nationale, 15 avril 2015, 2ème séance). On notera cependant que rien dans la loi ne prévoit un cadre pour ces négociations quant à ces « *points du réseau* » affectés. Dire cela dans le cadre du débat parlementaire, c'est confirmer que la loi n'a pas défini de conditions volumétriques, financières, matérielles et techniques, de mise en œuvre des moyens de surveillance.

Dès lors, l'affirmation de Monsieur le Ministre de l'Intérieur, Bernard Cazeneuve, selon laquelle il n'y aura pas de « *Deep Packet Inspection* » n'est pas fondée puisque la loi, du fait même de son imprécision reconnue par le Gouvernement en séance publique devant l'Assemblée Nationale, rend parfaitement possible que les moyens d'accès appelés « boîtes noires » soient connectées sur les cœurs de réseaux.

Au regard de ce flou majeur au sujet de la notion de « réseaux » dans le présent texte, il s'ensuit que tout équipement ou installation de tout fournisseur pourrait être concerné (i.e. requis pour mettre en place une sonde ou « boite noire ») par les mesures de surveillance dès lors qu'il constitue une partie d'un réseau. Ce périmètre extrêmement large susceptible d'être concerné par les opérations de surveillance apparaît manifestement excessif par rapport à l'objectif poursuivi, puisqu'il écarte toute exigence - et rend impossible, *a priori* ou a *posteriori* - tout contrôle de pertinence ni de proportionnalité.

En conséquence, l'absence de précision de la loi viole le principe de clarté et d'intelligibilité de la loi et l'article 34 de la Constitution.

**VI.3.** En second lieu, force est d'admettre que si la définition de réseau retenue devait être celle de l'article L. 32 du CPCE, dont on a vu la portée immense -en réalité, indéfinie-, la

disproportion manifeste entre le but poursuivi et les moyens mis en œuvre n'en serait que plus flagrante.

Alors que la critique de surveillance de masse a été écartée par le Gouvernement comme étant non fondée, il est certain que le placement de sondes algorithmiques sur une multitude de points d'accès aux réseaux constitue, par nature, une collecte indifférenciée de données et de métadonnées, dont on a vu qu'elles révèlent beaucoup de la vie privée et sociale des individus. De surcroit, cette collecte massive ne garantit pas l'efficacité des opérations de prévention, puisque l'enjeu d'efficacité repose sur la capacité à stocker et exploiter une quantité inédite d'informations et de documents, dont seule une analyse tout autant massive permettra d'en tirer des conséquences pour anticiper, empêcher et stopper des attaques terroristes ou d'autres menaces telles que visées par le législateur.

Comme l'a relevé l'Inria dans une note rendue publique (voir Production jointe), les statistiques liés à l'usage d'algorithmes conduit nécessairement à une surveillance massive pour détecter les potentiels terroristes. Ainsi est-il écrit dans le paragraphe relatif au *« paradoxe des faux positifs »* que *« tout algorithme de détection a une marge d'erreur c'est à dire va identifier des personnes sans intention terroriste (des « faux-positifs »). Si la marge d'erreur est de 1%, ce qui est considéré à ce jour comme très faible, l'algorithme identifiera quelques 600 000 personnes sur une population totale de 60 millions de personnes. Si le nombre de vrais terroristes est par exemple de 60, ces vrais terroristes ne représenteront que 0,01% de la population identifiée »*. S'ensuit un développement sur la nécessité de croiser un maximum d'informations de façon extrêmement intrusive aux fins de réaliser au mieux l'objectif de prévention poursuivi et sur les limites technologiques de l'anonymisation (Production jointe).

Nul doute ici que la pose de sondes algorithmiques se heurterait dans ces conditions à votre jurisprudence déployée sur le terrain de la disproportion manifeste (voir en particulier la décision du 16 juillet 1996 et la censure d'une disposition étendant la procédure de perquisition du domicile privé sous le contrôle de l'autorité judiciaire, précitée) et celles que la Cour Européenne des Droits de l'Homme et la Cour de Justice de l'Union Européenne ont récemment confirmé sur le terrain de la protection des libertés fondamentales, dont la protection de la vie privée fait partie. Ainsi que l'a relevé la CJUE, « *ces données prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la personne dont les données ont été conservées, telles que les habitudes de vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci* » (CJUE Grande Chambre, précité, § 27 et s.).

C'est en vain qu'il serait argué que l'article L. 851-3 nouveau du CSI prévoit que ces traitements automatisés de recueil d'informations sont paramétrés de façon à éviter des collectes indues et à s'assurer de l'anonymat des personnes concernées. D'abord, la note précise de l'Inria est particulièrement claire sur ce point et montre que cette garantie n'est que virtuelle et ne permettra pas de protéger les citoyens d'une surveillance injustifiée et personnelle, et qui ne manquerait pas de porter atteinte à la confiance dans les outils et technologies numériques que défendent nos associations professionnelles. Ensuite, l'ensemble de la communauté scientifique

considère illusoire que de telles sondes puissent être ainsi cantonnées dans leurs effets dès lors que l'absence de prédétermination de la cible – à l'inverse de l'hypothèse prévue par l'article L. 851-2 nouveau du CSI évoquant du recueil d'information en temps réel d'une personne préalablement identifié comme présentant une menace – oblige à une collecte très large de données pour obtenir, puisque tel est bien le but, les connexions révélant des probabilités de préparation d'actes terroristes.

En outre, c'est ignorer que l'ensemble des Etats membres de l'Union européenne entendent par une donnée « anonyme » ou « anonymisée ». L'analyse des techniques ou situations d'anonymat réalisée par ces autorités nationales de contrôle indépendant, repose sur des études réglementaires et techniques internationales, notamment européennes et américaines. Cette analyse précise, publiée en avril 2014, résulte de deux décisions parfaitement adaptées à la matière[1]-[2]. Elle établit clairement que les métadonnées visées par la loi sur le renseignement n'ont, y compris lorsqu'elles sont collectées par des sondes algorithmiques, absolument aucun caractère d'anonymat intrinsèque. Elles ne constituent, s'agissant de leur imputabilité à des personnes physiques identifiables, que des « données pseudonymes » au sens du projet de règlement européen sur la protection des données personnelles en cours d'adoption, c'est-à-dire des *« données indirectement nominatives »* au sens originel qu'en avait donné le législateur français en adoptant la loi n°78-17.

Ces données qu'il s'agira de collecter et d'analyser massivement relèvent, sans aucun doute sérieux, de la protection de la vie privée résultant de l'article 2 de la Déclaration des Droits de l'Homme et du Citoyen de 1789.

Ces dispositions aboutissent donc à des mécanismes dont l'impact est manifestement disproportionné au regard de l'objectif de la loi et des droits et libertés fondamentaux constitutionnellement garantis dont le droit à la vie privée et à la liberté personnelle.

La censure est certaine de tous ces chefs.

## VII. Sur l'article 6 de la loi et les mesures de surveillance internationale

La loi critiquée crée un Chapitre IV dans le code de la sécurité intérieure rendant possible la mise en œuvre de procédés de recueil d'information et de renseignements s'agissant de communications qui sont émises ou reçues à l'étranger.

Il est pourtant évident que la Constitution française a vocation à régir les termes de la loi française et les missions de police administrative qu'elle confie aux services français de renseignement, afin de protéger les libertés individuelles et collectives des ressortissants français, que ces derniers communiquent à destination de l'étranger ou depuis un territoire étranger.

[1] Avis 04/2014 sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_fr.pdf

[2] Avis 05/2014 sur les Techniques d'anonymisation - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf

L'article L. 854.1 nouveau du CSI est rédigé de façon si imprécise que la méconnaissance du principe de clarté et d'intelligibilité de la loi et ensemble de l'article 34 de la Constitution est flagrante.

Ces mesures sont prévues sans qu'aucun détail même *a minima* ne soit donné sur les critères concernant le périmètre et les conditions de mise en œuvre des moyens de renseignement dans une telle situation. Certes un décret en Conseil d'Etat sera pris après avis de la CNCTR et apportera quelques précisions, mais ce texte ne sera pas publié, en sorte que l'absence de précision dans la loi et de publication du Décret censé les expliciter défie l'objectif constitutionnel destiné à éviter toute forme d'arbitraire dans l'interprétation des textes et tout particulièrement quand sont en cause les droits et libertés fondamentaux y compris des ressortissants français circulant ou établis à l'étranger.

Rien ne justifie ici que les conditions de mise en œuvre de ces techniques soient moins protectrices que l'ensemble du dispositif, dont on a vu qu'il était déjà entaché de plusieurs inconstitutionnalités, alors même que les entreprises françaises sont établies dans la plupart des pays du monde et emploient ou dépêchent à l'étranger des dizaines de milliers de citoyens français. Ces citoyens de la République française pourraient-ils être moins bien protégés par la loi, au motif qu'ils communiquent depuis l'étranger ou qu'ils reçoivent des communications depuis notre territoire national ? En prévoyant ici une dégradation supplémentaire des garanties, du fait des imprécisions de ce dispositif, le législateur est manifestement resté en deçà de sa propre compétence.

La censure du dispositif ne manquera pas d'intervenir.

*  *

**Par ces motifs** et tous autres à déduire, suppléer ou relever même d'office, les associations signataires ont donc l'honneur, Monsieur le Président, Mesdames et Messieurs les membres du Conseil Constitutionnel, de vous demander de censurer les dispositions ainsi contraires à la Constitution.

**PJ** :

- Note de l'Inria

- Avis 04/2014 sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_fr.pdf )

- Avis 05/2014 sur les Techniques d'anonymisation (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf)