Conseil constitutionnel

AMICUS CURIÆ

transmis au Conseil constitutionnel dans le cadre des saisines visant la
« loi relative au renseignement »

PAR

1. **French Data Network (Réseau de données français)**, dite FDN.
   Association régie par la loi du 1er juillet 1901 établie 16 rue de Cachy, 80090 Amiens, enregistrée en préfecture de la Somme sous le numéro W751107563, opérateur déclaré auprès de l'ARCEP sous la référence 07/1149, prise en la personne de son président M. Fabien Sirjean.
   Tél. : 06 36 18 91 00
   Mail : `president@fdn.fr` / `buro@fdn.fr`
2. **La Quadrature du Net**
   Association régie par la loi du 1er juillet 1901 établie au 60 rue des Orteaux 75019, Paris, enregistrée en préfecture de police de Paris sous le numéro W751218406, prise en la personne de son président M. Philippe Aigrain.
   Tél. : 06 73 60 88 43
   Mail : `contact@laquadrature.net`
3. **Fédération des fournisseurs d'accès à Internet associatifs**, dite Fédération FDN (FFDN).
   Fédération régie par la loi du 1er juillet 1901 établie 16 rue de Cachy, 80090 Amiens, enregistrée en préfecture de la Somme sous le numéro W751210904, regroupant 27 fournisseurs d'accès associatifs français, déclarés auprès de l'ARCEP, et un fournisseur d'accès associatif belge déclaré auprès du régulateur, prise en la personne de son président M. Benjamin Bayart.
   Tél. : 06 60 24 24 94
   Mail : `contact@ffdn.org`

Le 29 juin 2015

Disponible en PDF en ligne
`http://x.fdn.fr/amicus`

Résumé

La loi relative au renseignement introduit un cadre juridique régissant l'ensemble des activités des services de renseignement, et notamment la surveillance secrète des communications électroniques. Le législateur et le gouvernement ont cependant échoué à assurer une conciliation juste et proportionnée entre la poursuite des objectifs affichés et le respect des droits et libertés protégés par la Constitution, et en particulier le droit à la vie privée et la liberté de communication.

D'abord, cette loi révèle en de nombreux points cruciaux une inintelligibilité patente ; qu'il s'agisse des principes centraux relatifs aux finalités poursuivies par les services de renseignement ou encore de la notion d'« information ou documents » traités par les réseaux des opérateurs ou les services de prestataires par lesquels transitent les communications électroniques de la totalité de la population.

Ensuite, plusieurs des techniques autorisées se révèlent particulièrement attentatoires aux droits et libertés, sans permettre effectivement d'atteindre les objectifs poursuivis ni être suffisamment encadrées ou définies.

Enfin, l'activité des services est soumise au contrôle ineffectif d'une commission, là où seules les garanties d'une juridiction auraient pu répondre aux exigences constitutionnelles, et alors qu'aucune procédure de signalement des abus n'est prévue, tandis que la procédure contentieuse créée est largement illusoire.

Les associations *amicus* apportent de nombreux éclairages techniques afin de restituer le contexte de la mise en œuvre de cette loi [1]. Compte tenu non seulement de la démocratisation de l'accès à Internet, mais aussi de la diversité et de l'intensité de ses usages politiques, sociaux et économiques, ces éclairages permettent de mieux saisir la gravité exceptionnelle des atteintes que porte la loi déférée aux droits et libertés publiques constitutionnellement protégés, notamment au titre de la Déclaration des droits de l'Homme et du citoyen de 1789. Ils contribuent ainsi à montrer que, du moins sur certains points, l'évolution des techniques et de leurs usages requiert un changement de doctrine de la part des juges constitutionnels dans l'encadrement des activités de surveillance secrète.

1. Voir en particulier : chapitre 5 page 31 ; chapitre 6 page 47 ; chapitre 7 page 53 ; chapitre 9 page 69.

Présentation du plan

Après une présentation des associations à l'origine du présent document (chapitre 1 page 9) et une brève description du contexte dans lequel cette loi a été adoptée (chapitre 2 page 11), il sera démontré que les dispositions de la loi déférée échouent à répondre à de nombreuses exigences constitutionnelles.

Les moyens soulevés sont les suivants :

Premièrement, les finalités prévues à l'article L. 811-3 pour la poursuite desquelles les techniques de surveillance peuvent être mises en œuvre rendent celles-ci manifestement disproportionnées quand elles ne sont pas parfaitement inintelligibles (chapitre 3 page 15).

Deuxièmement, les services autorisés à mettre en œuvre les techniques de renseignement ne sont pas définis par la loi, cette dernière échouant ainsi à encadrer les risques d'abus et de dysfonctionnement (chapitre 4 page 29).

Troisièmement, la notion d'« informations ou documents » désignant les données collectées par trois techniques de renseignement est manifestement inintelligible, alors même qu'elle conduit à des atteintes d'une gravité particulière (chapitre 5 page 31).

Quatrièmement, les communications chiffrées semblent être l'objet de suspicions particulières et de régimes dérogatoires alors même que leur usage est recommandé par diverses institutions publiques (chapitre 6 page 47).

Cinquièmement, les « boîtes noires algorithmiques » prévues à l'article L. 851-3 permettent de porter une atteinte indiscriminée aux droits et libertés de l'ensemble de la population, se révélant particulièrement peu efficaces pour lutter contre le terrorisme et contraires à deux directives de l'Union européenne (chapitre 7 page 53).

Sixièmement, les techniques de captation d'images, de paroles et de données privées prévues aux articles L. 853-1 et L. 853-2 se fondent sur des critères inintelligibles (chapitre 8 page 63).

Septièmement, les régimes spéciaux résultant de l'article 854-1 relatif aux mesures de « surveillance internationale » posent plusieurs problèmes liés à l'inintelligibilité de la loi, aux graves insuffisances du contrôle exercé sur ces mesures, ainsi qu'à la remise en cause de l'universalité des droits affirmée à la fois à l'article premier de la Déclaration de 1789 et dans le bloc de conventionnalité (chapitre 9 page 69).

Huitièmement, l'absence de contrôle indépendant et effectif des techniques autorisées, tant préalablement (chapitre 10 page 85) que postérieurement (chapitre 11 page 105) à leur mise en œuvre, rend l'ensemble du dispositif contraire à la Constitution.

Enfin, l'aggravation des sanctions prévues pour les délits de fraude informatique constitue un cavalier législatif (chapitre 12 page 121).

0. Table des matières

Première partie

INTRODUCTION

1. Présentation

1.1. French Data Network

FDN est une association loi 1901 et un fournisseur d'accès à Internet. Elle existe et exerce son activité depuis 1992, ce qui en fait le plus ancien fournisseur d'accès français à Internet encore en activité. Regroupant 450 adhérents, FDN est administrée de manière entièrement bénévole. Elle ne fournit d'accès à Internet qu'à ses membres.

L'association est donc concernée par la loi déférée à double titre. En tant que fournisseur d'accès à Internet, la mise en œuvre de nouvelles mesures attentatoires aux droits et libertés fondamentaux pourrait lui être imposée sans garanties contre l'arbitraire.

FDN est également concernée en tant qu'association, représentant ses membres, y compris ceux auxquels elle fournit un accès à Internet. Ses abonnés sont concernés au premier chef par les mesures restrictives de droits ou de libertés mises en œuvre par la loi déférée et les autres membres de l'association sont concernés en tant qu'internautes, même si leur accès n'est pas fourni par l'association.

1.2. La Quadrature du Net

La Quadrature du Net est une association loi 1901. Son objet général est la défense des droits fondamentaux dans l'environnement numérique. À ce titre, elle intervient dans les débats politiques, juridiques et techniques touchant à Internet, aux niveaux français et européen. Dans le champ du droit, et outre les recours contentieux, La Quadrature du Net défend les libertés publiques et les droits fondamentaux à travers des analyses juridiques ou en proposant et en évaluant des amendements au cours des procédures législatives (ce qu'elle a fait au cours de l'examen parlementaire de la loi déférée). L'un des axes forts de ses positions est la défense d'une protection judiciaire des droits fondamentaux sur Internet, et notamment la liberté d'expression, la liberté de communication ainsi que le droit au respect de la vie privée.

1.3. Fédération des fournisseurs d'accès à Internet associatifs

La Fédération FDN regroupe 28 fournisseurs d'accès à Internet associatifs, dont 27 sont des associations de droit français (loi de 1901 ou droit spécifique d'Alsace Moselle, selon le cas), la 28^{e} étant une association de droit belge. Toutes ces associations sont gérées de manière bénévole et représentent, ensemble, plus de 2000 adhérents. FDN est une des associations membres, et fondatrice, de la Fédération FDN. Les associations membres de la Fédération FDN sont toutes signataires d'une charte par laquelle elles prennent des engagements éthiques et techniques.

Récemment, les trois associations ont introduit un recours pour excès de pouvoir devant le Conseil d'État contre le décret n^{o} 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion, publié au Journal officiel de la République française n^{o} 298 du 24 décembre 2014, p. 22224. Dans le cadre de cette procédure, les associations requérantes ont introduit une question prioritaire de constitutionnalité portant sur les articles L. 246-1 à L. 246-5 du code de la sécurité intérieure et transmise au Conseil constitutionnel (décision du Conseil d'État n^{o} 388 134 du 5 juin 2015). Cette transmission a depuis été enregistrée le 5 juin 2015 au registre du secrétariat général du Conseil constitutionnel sous le numéro 2015-478 QPC.

2. De l'affaire Snowden à la loi française sur le renseignement

Depuis le mois de juin 2013, les révélations sur les pratiques de surveillance des services de renseignement de la *National Security Agency* américaine (NSA) et de ses partenaires internationaux [1] suscitent une large controverse au niveau mondial. Il s'ensuit des débats juridiques nombreux et complexes sur l'illégalité de ces pratiques d'exception dans l'État de droit et leur compatibilité avec le principe même de démocratie. Plusieurs décisions majeures ont d'ailleurs été rendues ces derniers mois par des juridictions nationales ou internationales pour réformer le cadre applicable aux politiques de sécurité dans un sens plus protecteur des droits et libertés.

C'est dans ce contexte historique déterminant que la loi sur le renseignement, aujourd'hui déférée devant le Conseil constitutionnel, a été adoptée par le Parlement.

En France, les services de renseignement n'ont jamais disposé d'un cadre juridique adapté. Cette situation a permis le développement d'activités de surveillance des communications dans la plus grande opacité et, le plus souvent, dans l'illégalité. Personne ne conteste qu'une loi définissant et encradrant le renseignement était donc nécessaire. Cependant, après les attentats de Paris, en janvier dernier, le Gouvernement a fait du projet de loi sur le renseignement sa principale réponse politique à ces événements tragiques, arguant de la lutte contre le terrorisme pour procéder à un élargissement sans précédent des compétences et outils octroyés aux services de renseignement, bien au-delà de la seule question terroriste. Sans même ouvrir de véritable débat sur les failles du dispositif français en la matière, le Gouvernement s'est ainsi livré à une opération de blanchiment législatif des illégalités existantes, tandis que l'argument de l'urgence et le choix de la procédure accélérée contribuaient à inhiber le débat public.

Les quelques garanties et mécanismes de contrôle inscrits dans le texte ne suffisent guère à assurer le droit à la sûreté, le droit au respect de la vie privée et la liberté de communication. En dépit des nombreuses critiques émanant d'organisations de défense des droits dans l'environnement numérique, des organisations internationales de défense des droits de l'Homme, de syndicats de juges, d'avocats, de journalistes, de policiers, d'associations de victimes de terrorisme, d'associations de travailleurs sociaux et d'acteurs du numérique ; en dépit des dénonciations de la CNIL, de la CNCDH, mais aussi du commissaire aux droits de l'Homme du Conseil de l'Europe ou des rapporteurs de l'ONU

1. *Inter alia* le Government Communications Headquarters britannique (GCHQ), la Direction générale de la sécurité extérieure française (DGSE) et le Bundesnachrichtendienst allemand (BND).

et de l'OSCE, le législateur n'a pour sa part procédé qu'à des amendements souvent superficiels qui échouent à répondre aux principaux dangers de ce texte.

Aujourd'hui, en France comme ailleurs en Europe et dans le monde, c'est aux juges que revient le rôle de garant *en dernier ressort* des droits fondamentaux et des libertés publiques. Face à la banalisation de la surveillance généralisée qu'illustre la présente loi, face à l'inertie d'un pouvoir politique complice d'une véritable fuite en avant de la raison d'État, nos associations comptent sur le Conseil constitutionnel pour se montrer à la hauteur du défi historique auquel est confronté l'État de droit.

Ce document constitue une modeste contribution à sa réflexion. Dans cet *amicus curiæ*, nous montrons que la mise en œuvre de ce texte de loi aboutirait à de multiples violations de la Constitution française ainsi que du droit européen et international applicable aux activités de surveillance et de renseignement.

Deuxième partie

CHAMP DES TECHNIQUES AUTORISÉES

3. Finalités autorisant le recours aux techniques de renseignement

L'article 2 de la loi déférée insère un article L. 811-3 au code de la sécurité intérieure (CSI) prévoyant les neuf finalités dont la poursuite autorise le recours aux techniques de renseignement prévues par cette loi et ainsi rédigé :

> *« **Article L. 811-3.***
> *« Pour le seul exercice de leurs missions respectives, les services spécialisés de renseignement peuvent recourir aux techniques mentionnées au titre V du présent livre pour le recueil des renseignements relatifs à la défense et à la promotion des intérêts fondamentaux de la Nation suivants :*
> *« 1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ;*
> *« 2° Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ;*
> *« 3° Les intérêts économiques, industriels et scientifiques majeurs de la France ;*
> *« 4° La prévention du terrorisme ;*
> *« 5° La prévention :*
> *« a) Des atteintes à la forme républicaine des institutions ;*
> *« b) Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ;*
> *« c) Des violences collectives de nature à porter gravement atteinte à la paix publique ;*
> *« 6° La prévention de la criminalité et de la délinquance organisées ;*
> *« 7° La prévention de la prolifération des armes de destruction massive. »*

Outre le fait de ne pas respecter l'objectif d'intelligibilité de la loi, la vaste définition de ces finalités implique, pour y répondre, la mise en place de procédures et la mise en œuvre de mesures techniques disproportionnées avec le sujet.

3.1. Des finalités porteuses de disproportion

La présente loi autorise sept techniques de renseignement dès lors qu'elles poursuivent l'une des finalités énoncées à l'article L. 811-3 :

1. le recueil auprès d'opérateurs et d'hébergeurs d'informations ou documents portant sur des communications électroniques (nouvel article L. 851-1 du CSI) ;

2. le recueil en temps réel auprès des mêmes personnes de données techniques permettant la localisation d'un terminal — d'un ordinateur ou d'un téléphone (L. 851-4) ;
3. l'utilisation d'un dispositif technique permettant la localisation en temps réel d'une personne, d'un véhicule ou d'un objet, avec la possibilité de s'introduire dans un lieu privé ou un véhicule pour le poser (L. 851-5) ;
4. le recueil, au moyen d'un dispositif technique de proximité, de données techniques permettant l'identification et la localisation d'un terminal et de son utilisateur (L. 851-6) ;
5. l'interception des correspondances électroniques d'une personne et de toutes celles de son entourage susceptibles de fournir des informations utiles à la finalité poursuivie (L. 852-1) ;
6. l'utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel, ou d'images dans un lieu privé, notamment d'habitation (L. 853-1) ;
7. l'utilisation d'un dispositif technique collectant et transmettant des informations contenues ou entrant sur un ordinateur ou celles auxquelles accède son utilisateur, avec la possibilité de s'introduire dans un lieu privé pour le poser (L. 853-2).

Toutes ces techniques portent manifestement atteinte au droit au respect de la vie privée ou à l'inviolabilité du domicile, garantis par l'article 2 de la Déclaration de 1789.

Pour que de telles atteintes soient légales, le Conseil constitutionnel exige du législateur, en vertu de l'article 34 de la Constitution, qu'il fixe « 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, n° 2004-492 DC du 02 mars 2004, cons. 75 et 76).

Or, pour trois des neuf finalités de l'article L. 811-3, le législateur a manifestement échoué à réaliser une telle conciliation.

3.1.1. Défense et promotion des intérêts économiques, industriels et scientifiques majeurs de la France

La notion d'« intérêts économiques, industriels et scientifiques majeurs de la France » n'est définie par aucune disposition constitutionnelle ou légale. Dès lors, une telle finalité justifierait la surveillance de toute personne dont le comportement est simplement susceptible de nuire à la promotion des intérêts individuels, privés, de virtuellement n'importe quelle entreprise française ; elle est ainsi manifestement disproportionnée au regard des atteintes faites aux droits et libertés fondamentaux de ces personnes.

Par ailleurs, la démission du législateur de son rôle d'encadrement de l'action des services de renseignement est nettement révélée par sa modification faite de la formulation de cette finalité. Alors que le projet initial visait les « intérêts économiques et scientifiques *essentiels* de la France », il s'agit dans la loi déférée des « intérêts économiques, industriels et scientifiques *majeurs* de la France », notion autrement plus large.

En conclusion,

Le 3° de l'article L. 811-3 inséré au CSI par la loi déférée est entaché d'incompétence négative, le législateur ayant manqué à l'obligation que lui impose l'article 34 de la Constitution d'assurer, en vue de l'article 2 de la Déclaration de 1789, la juste conciliation entre les intérêts qu'il défend et le respect des droits et libertés fondamentaux de citoyens, et doit ainsi être censuré.

Subsidiairement,

La notion d'« intérêts économiques, industriels et scientifiques majeurs de la France » peut être interprétée comme limitée à des enjeux de défense et de sécurité, comme le sont la majorité des intérêts fondamentaux de la Nation énoncés par le présent article et tels que le justifierait l'ampleur des atteintes permises par la présente loi.

Ainsi considérée, cette notion serait comprise dans le champ limité donné par le législateur de la « défense économique », au titre III du livre III du code de la défense, et particulièrement à son chapitre II, intitulé « Protection des installations d'importance vitale ».

L'objet de cette défense économique est défini à l'article L. 1332-1 de ce code comme couvrant « les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation ».

La défense et la promotion des « intérêts économiques, industriels et scientifiques majeurs de la France » consisteraient dès lors à empêcher l'« indisponibilité » des éléments visés à cet article.

Ainsi, la finalité définie au 3° de l'article examiné pourrait être interprétée comme signifiant « prévenir l'indisponibilité des établissements, installations et ouvrages visés à l'article L. 1332-1 du code de la défense ». Sous cette réserve seulement, la finalité énoncée par cette disposition ne serait pas manifestement contraire à la Constitution.

3.1.2. Prévention de la criminalité et de la délinquance organisées

La liste des infractions visées par la formule « criminalité et de la délinquance organisées » est faite au titre XXV, intitulé « De la procédure applicable à la criminalité et à la délinquance organisées », du livre IV du code de procédure pénale, qui prévoit que :

> *« **Article 706-73***
> *« La procédure applicable à l'enquête, la poursuite, l'instruction et le jugement des crimes et des délits suivants est celle prévue par le présent code, sous réserve des dispositions du présent titre :*
> *« 1° Crime de meurtre commis en bande organisée prévu par le 8° de l'article 221-4 du code pénal ;*
> *« 2° Crime de tortures et d'actes de barbarie commis en bande organisée prévu par l'article 222-4 du code pénal ;*
> *« 3° Crimes et délits de trafic de stupéfiants prévus par les articles 222-34 à 222-40 du code pénal ;*

« 4° Crimes et délits d'enlèvement et de séquestration commis en bande organisée prévus par l'article 224-5-2 du code pénal ;

« 5° Crimes et délits aggravés de traite des êtres humains prévus par les articles 225-4-2 à 225-4-7 du code pénal ;

« 6° Crimes et délits aggravés de proxénétisme prévus par les articles 225-7 à 225-12 du code pénal ;

« 7° Crime de vol commis en bande organisée prévu par l'article 311-9 du code pénal ;

« 8° Crimes aggravés d'extorsion prévus par les articles 312-6 et 312-7 du code pénal ;

« 8° bis Délit d'escroquerie en bande organisée prévu par le dernier alinéa de l'article 313-2 du code pénal ;

« 9° Crime de destruction, dégradation et détérioration d'un bien commis en bande organisée prévu par l'article 322-8 du code pénal ;

« 10° Crimes en matière de fausse monnaie prévus par les articles 442-1 et 442-2 du code pénal ;

« 11° Crimes et délits constituant des actes de terrorisme prévus par les articles 421-1 à 421-6 du code pénal ;

« 12° Délits en matière d'armes et de produits explosifs commis en bande organisée, prévus par les articles L. 2339-2, L. 2339-3, L. 2339-10, L. 2341-4, L. 2353-4 et L. 2353-5 du code de la défense ainsi que par les articles L. 317-2, L. 317-4 et L. 317-7 du code de la sécurité intérieure ;

« 13° Délits d'aide à l'entrée, à la circulation et au séjour irréguliers d'un étranger en France commis en bande organisée prévus par l'article L622-1 du code de l'entrée et du séjour des étrangers et du droit d'asile ;

« 14° 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 même code, du produit, des revenus, des choses provenant des infractions mentionnées aux 1° à 13° ;

« 15° Délits d'association de malfaiteurs prévus par l'article 450-1 du code pénal, lorsqu'ils ont pour objet la préparation de l'une des infractions mentionnées aux 1° à 14° et 17° ;

« 16° Délit de non-justification de ressources correspondant au train de vie, prévu par l'article 321-6-1 du code pénal, lorsqu'il est en relation avec l'une des infractions mentionnées aux 1° à 15° et 17° ;

« 17° Crime de détournement d'aéronef, de navire ou de tout autre moyen de transport commis en bande organisée prévu par l'article 224-6-1 du code pénal ;

« 18° Crimes et délits punis de dix ans d'emprisonnement, contribuant à la prolifération des armes de destruction massive et de leurs vecteurs entrant dans le champ d'application de l'article 706-167 ;

« 19° Délit d'exploitation d'une mine ou de disposition d'une substance concessible sans titre d'exploitation ou autorisation, accompagné d'atteintes à l'environnement, commis en bande organisée, prévu à l'article L. 512-2 du code minier, lorsqu'il est connexe avec l'une des infractions mentionnées aux 1° à 17° du présent article ;

« 20° Délits de dissimulation d'activités ou de salariés, de recours aux services d'une personne exerçant un travail dissimulé, de marchandage de main-d'œuvre, de prêt illicite de main-d'œuvre, d'emploi d'étrangers sans titre de travail prévus aux 1° et 3° de l'article L. 8221-1 et aux articles L. 8221-3, L. 8221-5, L. 8224-1, L. 8224-2, L. 8231-1, L. 8234-1, L. 8234-2, L. 8241-1, L. 8243-1, L. 8243-2, L. 8251-1 et L. 8256-2 du code du travail.

« Pour les infractions visées aux 3°, 6° et 11°, sont applicables, sauf précision contraire, les dispositions du présent titre ainsi que celles des titres XV, XVI et XVII. »

Cette liste est particulièrement large.

Certes, elle comprend des crimes particulièrement graves — tels que le meurtre ou la torture — commis en bande organisée, pouvant justifier des mesures de surveillance ; mais cette liste comprend aussi certains délits moins graves et commis par des personnes seules, par exemple « le transport, la détention, l'offre, la cession, l'acquisition ou l'emploi illicites de stupéfiants », prohibés à l'article 222-37 du code pénal auquel renvoie directement l'article 706-73 du code de procédure pénale.

Or, la mise en œuvre des techniques de renseignement instituées par la présente loi n'est pas nécessaire pour la poursuite de ces objectifs visés par le législateur ; en outre cette finalité est manifestement trop large pour qu'un équilibre puisse être assuré avec les atteintes aux droits et libertés constitutionnellement protégés.

En conclusion,

Le 6° de l'article L. 811-3 inséré au CSI par la loi déférée est entaché d'incompétence négative, le législateur ayant manqué à l'obligation que lui incombe l'article 34 de la Constitution d'assurer, en vue de l'article 2 de la Déclaration de 1789, la juste conciliation entre les intérêts qu'il défend et le respect des droits et libertés fondamentaux de citoyens, et doit ainsi être censuré.

3.1.3. Exécution des engagements européens et internationaux de la France

Considérée en tant que telle, la notion d'« engagements européens et internationaux de la France » couvre tout acte conclu entre la France et un ou plusieurs pays tiers ainsi que tout acte de l'Union européenne, quel qu'en soit l'objet. Dès lors, une telle formule conduit la présente loi à autoriser des techniques de renseignement pour la poursuite d'objectifs qui, manifestement, pour nombre des engagements européens et internationaux de la France, ne sauraient nullement justifier les atteintes réalisées.

Par exemple, il est manifestement injustifié que puissent être autorisées selon la présente loi des mesures de surveillance visant des citoyens pour la seule raison que ceux-ci seraient susceptibles de nuire à la réalisation des objectifs des traités internationaux concernant la compétence judiciaire et l'exécution des décisions en matière civile et commerciale [1], ou concernant les changements climatiques [2], la biodiversité [3], le droit d'auteur [4] ou le droit de timbre en matière de chèques [5].

En conclusion,

De par son expression « l'exécution des engagements européens et internationaux de la France », le 2° de l'article L. 811-3 créé par la loi déférée est entaché d'incompétence négative, le législateur ayant manifestement manqué à l'obligation que lui incombe l'article

1. Convention de la Haye du 1er mars 1954 relative à la procédure civile, Convention de Bruxelles du 27 septembre 1968 concernant la compétence judiciaire et l'exécution des décisions en matière civile et commerciale, Convention de Lugano du 16 septembre 1988 concernant la compétence judiciaire et l'exécution des décisions en matière civile et commerciale
2. Convention cadre des Nations Unies de New-York du 9 mai 1992 sur les changements climatiques
3. Convention de Rio du 5 juin 1992 sur la diversité biologique
4. Convention universelle du 24 juillet 1971 sur le droit d'auteur
5. Convention de Genève du 19 mars 1931 relative au droit de timbre en matière de chèques

34 de la Constitution d'assurer, en vue de l'article 2 de la Déclaration de 1789, la juste conciliation entre les intérêts qu'il défend et le respect des droits et libertés fondamentaux de citoyens, et doit ainsi être censuré.

3.2. Des finalités inintelligibles et inaccessibles

Depuis 1999, de jurisprudence constante, le Conseil constitutionnel considère comme contraires aux articles 4, 5, 6 et 16 de la Déclaration de 1789 les normes dont « *les citoyens ne disposent pas d'une connaissance suffisante* » (Décision n° 99-421 DC, 16 décembre 1999, cons. 13).

Il en a depuis dégagé un objectif de valeur constitutionnelle d'intelligibilité et d'accessibilité de la loi qui, avec l'obligation qu'a le législateur « *d'exercer pleinement la compétence que lui confie la Constitution et, en particulier, son article 34* », impose à ce dernier « *d'adopter des dispositions suffisamment précises et des formules non équivoques* » afin de « *prémunir les sujets de droit contre une interprétation contraire à la Constitution ou contre le risque d'arbitraire, sans reporter sur des autorités administratives ou juridictionnelles le soin de fixer des règles dont la détermination n'a été confiée par la Constitution qu'à la loi.* » (2006-540 DC, 27 juillet 2006, cons. 9 ; 2007-557 DC, 15 novembre 2007, cons. 19 ; 2008-564 DC, 19 juin 2008, cons. 25 ; 2008-567 DC, 24 juillet 2008, cons. 39 ; 2013-685 DC, 29 décembre 2013, cons. 88)

Il sanctionne ainsi l'incompétence négative du législateur qui, pour n'avoir pas épuisé la compétence que lui confère l'article 34 de la Constitution, échoue à produire des normes suffisamment précises et non équivoques, que le Conseil censure (voir, par ex. la décision n° 2004-499 DC du 29 juillet 2004, cons. 9, 11 et 12).

Plus précisément, le Conseil constitutionnel a pu relever plusieurs critères caractérisant le défaut d'intelligibilité et d'accessibilité des lois soumises à son examen, tels que :

- le caractère équivoque d'une formule « *susceptible d'au moins deux interprétations* » (85-191 DC, 10 juillet 1985, cons. 5) ;
- le caractère « ambiguë » d'une notion qui « *risquerait de créer la confusion dans l'esprit* » des citoyens (2003-475 DC, 24 juillet 2003, cons. 21 à 26)
- le caractère imprécis de formules qui « *pourraient faute de précisions suffisantes entraîner une atteinte à des droits et libertés constitutionnellement garantis qu'il appartient à la loi de sauvegarder* » et non au règlement, revenant « *au législateur de déterminer lui-même la nature des garanties nécessaires* » (85-198 DC, 13 décembre 1985, cons. 11 et 12) ;
- la « *complexité excessive [de règles] au regard de l'aptitude de leurs destinataires à en mesurer utilement la portée* » (2005-530 DC, 29 décembre 2005, cons. 77 à 89).

Or, pour trois des neuf finalités de l'article L. 811-3, le législateur a manifestement échoué à produire des normes intelligibles et accessibles.

3.2.1. Prévention des violences collectives de nature à porter gravement atteinte à la paix publique

Premièrement, la notion de « violences » est définie par la loi au paragraphe II, intitulé « des violences », de la section I du chapitre II du titre II du livre II du code pénal.

La notion de « violence collective » se retrouve sans équivoque parmi les infractions définies à ce paragraphe : il s'agit, d'une part, des infractions de violences définies aux articles 222-7 à 222-13 du code pénal lorsqu'elles s'accompagnent de la circonstance aggravante d'être commises « par plusieurs personnes agissant en qualité d'auteur ou de complice » et, d'autre part, des infractions de violences définies aux articles 222-14-1 et 222-14-2 — dont le caractère collectif est un des éléments constitutifs.

*« **Article 222-7***
« Les violences ayant entraîné la mort sans intention de la donner sont punies de quinze ans de réclusion criminelle.

*« **Article 222-8***
« L'infraction définie à l'article 222-7 est punie de vingt ans de réclusion criminelle lorsqu'elle est commise : [...]
« 8° Par plusieurs personnes agissant en qualité d'auteur ou de complice ; [...]

*« **Article 222-9***
« Les violences ayant entraîné une mutilation ou une infirmité permanente sont punies de dix ans d'emprisonnement et de 150 000 euros d'amende.

*« **Article 222-10***
« L'infraction définie à l'article 222-9 est punie de quinze ans de réclusion criminelle lorsqu'elle est commise : [...]
« 8° Par plusieurs personnes agissant en qualité d'auteur ou de complice ; [...]

*« **Article 222-11***
« Les violences ayant entraîné une incapacité totale de travail pendant plus de huit jours sont punies de trois ans d'emprisonnement et de 45 000 euros d'amende.

*« **Article 222-12***
« L'infraction définie à l'article 222-11 est punie de cinq ans d'emprisonnement et de 75 000 euros d'amende lorsqu'elle est commise : [...]
« 8° Par plusieurs personnes agissant en qualité d'auteur ou de complice ; [...]

*« **Article 222-13***
« Les violences ayant entraîné une incapacité de travail inférieure ou égale à huit jours ou n'ayant entraîné aucune incapacité de travail sont punies de trois ans d'emprisonnement et de 45 000 euros d'amende lorsqu'elles sont commises : [...]
« 8° Par plusieurs personnes agissant en qualité d'auteur ou de complice ; [...]

*« **Article 222-14-1***
« Lorsqu'elles sont commises en bande organisée ou avec guet-apens, les violences commises avec usage ou menace d'une arme sur un fonctionnaire de la police nationale, un

militaire de la gendarmerie, un membre du personnel de l'administration pénitentiaire ou toute autre personne dépositaire de l'autorité publique, ou sur un sapeur-pompier civil ou militaire ou un agent d'un exploitant de réseau de transport public de voyageurs dans l'exercice, à l'occasion de l'exercice ou en raison de ses fonctions ou de sa mission, sont punies :

« 1° De trente ans de réclusion criminelle lorsqu'elles ont entraîné la mort de la victime ;

« 2° De vingt ans de réclusion criminelle lorsqu'elles ont entraîné une mutilation ou une infirmité permanente ;

« 3° De quinze ans de réclusion criminelle lorsqu'elles ont entraîné une incapacité totale de travail pendant plus de huit jours ;

« 4° De dix ans d'emprisonnement et de 150 000 euros d'amende lorsqu'elles n'ont pas entraîné une incapacité totale de travail pendant plus de huit jours. [...]

*« **Article 222-14-2***

« Le fait pour une personne de participer sciemment à un groupement, même formé de façon temporaire, en vue de la préparation, caractérisée par un ou plusieurs faits matériels, de violences volontaires contre les personnes ou de destructions ou dégradations de biens est puni d'un an d'emprisonnement et de 15 000 euros d'amende. »

Secondement, la notion d'« atteinte à la paix publique » est aussi définie par la loi, au chapitre Ier, intitulé « des atteintes à la paix publique », du titre III du livre IV du code pénal.

Cette notion recouvre ainsi l'ensemble des infractions définies à ce chapitre, soit :

*« **Article 431-1***

« Le fait d'entraver, d'une manière concertée et à l'aide de menaces, l'exercice de la liberté d'expression, du travail, d'association, de réunion ou de manifestation ou d'entraver le déroulement des débats d'une assemblée parlementaire ou d'un organe délibérant d'une collectivité territoriale est puni d'un an d'emprisonnement et de 15 000 euros d'amende.

« Le fait d'entraver, d'une manière concertée et à l'aide de coups, violences, voies de fait, destructions ou dégradations au sens du présent code, l'exercice d'une des libertés visées à l'alinéa précédent est puni de trois ans d'emprisonnement et de 45 000 euros d'amende.

*« **Article 431-3***

« Constitue un attroupement tout rassemblement de personnes sur la voie publique ou dans un lieu public susceptible de troubler l'ordre public.

« Un attroupement peut être dissipé par la force publique après deux sommations de se disperser restées sans effet adressées dans les conditions et selon les modalités prévues par l'article L. 211-9 du code de la sécurité intérieure.

*« **Article 431-4***

« Le fait, pour celui qui n'est pas porteur d'une arme, de continuer volontairement à participer à un attroupement après les sommations est puni d'un an d'emprisonnement et de 15 000 € d'amende.

« L'infraction définie au premier alinéa est punie de trois ans d'emprisonnement et de 45 000 € d'amende lorsque son auteur dissimule volontairement en tout ou partie son visage afin de ne pas être identifié.

*« **Article 431-5***

« Le fait de participer à un attroupement en étant porteur d'une arme est puni de trois ans d'emprisonnement et de 45 000 € d'amende.

« Si la personne armée a continué volontairement à participer à un attroupement après les sommations, la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende.

« Si la personne armée dissimule volontairement en tout ou partie son visage afin de ne pas être identifiée, la peine est également portée à cinq ans d'emprisonnement et à 75 000 € d'amende.

*« **Article 431-6***

« La provocation directe à un attroupement armé, manifestée soit par des cris ou discours publics, soit par des écrits affichés ou distribués, soit par tout autre moyen de transmission de l'écrit, de la parole ou de l'image, est punie d'un an d'emprisonnement et de 15 000 euros d'amende.

« Lorsque la provocation est suivie d'effet, la peine est portée à sept ans d'emprisonnement et à 100 000 euros d'amende.

*« **Article 431-9***

« Est puni de six mois d'emprisonnement et de 7 500 euros d'amende le fait :

« 1° D'avoir organisé une manifestation sur la voie publique n'ayant pas fait l'objet d'une déclaration préalable dans les conditions fixées par la loi ;

« 2° D'avoir organisé une manifestation sur la voie publique ayant été interdite dans les conditions fixées par la loi ;

« 3° D'avoir établi une déclaration incomplète ou inexacte de nature à tromper sur l'objet ou les conditions de la manifestation projetée.

*« **Article 431-10***

« Le fait de participer à une manifestation ou à une réunion publique en étant porteur d'une arme est puni de trois ans d'emprisonnement et de 45 000 euros d'amende.

*« **Article 431-13***

« Constitue un groupe de combat, en dehors des cas prévus par la loi, tout groupement de personnes détenant ou ayant accès à des armes, doté d'une organisation hiérarchisée et susceptible de troubler l'ordre public.

*« **Article 431-14***

« Le fait de participer à un groupe de combat est puni de trois ans d'emprisonnement et de 45 000 euros d'amende.

*« **Article 431-15***

« Le fait de participer au maintien ou à la reconstitution, ouverte ou déguisée, d'une association ou d'un groupement dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées est puni de trois ans d'emprisonnement et de 45 000 euros d'amende.

« Lorsque l'association ou le groupement maintenu ou reconstitué est un groupe de combat au sens de l'article 431-14, la peine est portée à cinq ans d'emprisonnement et à 75 000 euros d'amende.

*« **Article 431-16***

« Le fait d'organiser un groupe de combat est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.

*« **Article 431-17***

« Le fait d'organiser le maintien ou la reconstitution, ouverte ou déguisée, d'un groupe de combat dissous en application de la loi du 10 janvier 1936 précitée est puni de sept ans d'emprisonnement et de 100 000 euros d'amende. »

En synthèse, la notion de « violences collectives de nature à porter gravement atteinte à la paix publique » résulte de la combinaison des notions de « violences collectives » et d'« atteinte à la paix publique » telles que définies par la loi, et couvre ainsi l'ensemble des infractions correspondant à chacune d'elles.

Or, parmi les infractions définies au chapitre intitulé « des atteintes à la paix publique » du code pénal et visées plus haut, une seule correspond à l'une des infractions de violences collectives définies au paragraphe intitulé « des violences » du code pénal et visées plus haut : l'infraction définie à l'article 431-1 du code pénal lorsqu'elle est constituée par des actes de violence, cet article disposant que :

« Le fait d'entraver, d'une manière concertée et à l'aide de menaces, l'exercice de la liberté d'expression, du travail, d'association, de réunion ou de manifestation ou d'entraver le déroulement des débats d'une assemblée parlementaire ou d'un organe délibérant d'une collectivité territoriale est puni d'un an d'emprisonnement et de 15 000 euros d'amende.

« Le fait d'entraver, d'une manière concertée et à l'aide de coups, violences, voies de fait, destructions ou dégradations au sens du présent code, l'exercice d'une des libertés visées à l'alinéa précédent est puni de trois ans d'emprisonnement et de 45 000 euros d'amende. »

Aucun des faits constitutifs des autres infractions définies par la loi comme « atteintes à la paix publique » ne correspond aux faits constitutifs des infractions définies par la loi comme « violences collectives ».

De sorte, la seule interprétation possible de la finalité de « prévention des violences collectives de nature à porter gravement atteinte à la paix publique » est celle de prévention du « fait d'entraver, d'une manière concertée et à l'aide de [violences contre les personnes], l'exercice de la liberté d'expression, du travail, d'association, de réunion ou de manifestation ou d'entraver le déroulement des débats d'une assemblée parlementaire ou d'un organe délibérant d'une collectivité territoriale ».

Or, cette interprétation ne découle certainement pas de la simple lecture de la formule choisie par le législateur. Par ailleurs, la complexité du rapport entre la formule choisie et son véritable sens ne saurait être justifiée par aucun impératif, et se révèle dès lors être excessive, le législateur aurait pu faire simplement référence au second alinéa de l'article 431-1 du code pénal ou employer une formule semblable à celle proposée ci-dessus sans autre conséquence que de produire un texte plus clair et accessible.

Dès lors, certaines des mesures de la présente loi ayant un impact sur les droits et libertés de l'ensemble des citoyens, la présente finalité, dont la poursuite autorise la réalisation de techniques de surveillance, présente une « complexité excessive au regard de

l'aptitude de [ses] destinataires à en mesurer utilement la portée », contrairement à ce que la Constitution exige de la loi (Déc. n° 2005-530 DC, 29 décembre 2005, cons. 77 à 89).

En conclusion,

Le 5°, c, de l'article L. 811-3 inséré au code de la sécurité intérieure par la loi déférée est entaché d'incompétence négative, le législateur ayant manqué à l'obligation que lui incombe l'article 34 de la Constitution de produire, en vue des articles 4, 5, 6 et 16 de la Déclaration de 1789, des normes intelligibles et accessibles, et doit ainsi être censuré.

Subsidiairement,

L'expression « violences collectives de nature à porter gravement atteinte à la paix publique » ici employée par le législateur doit être interprétée comme renvoyant uniquement à l'infraction définie au second alinéa de l'article 431-1 du code pénal lorsqu'elle est constituée par des violences telles que définies au paragraphe II, de la section I du chapitre II du titre II du livre II du code pénal.

Sous cette réserve seulement, la disposition en cause n'est pas manifestement contraire à l'objectif de valeur constitutionnelle d'intelligibilité et d'accessibilité de la loi et est conforme à la Constitution.

3.2.2. Défense et promotion des intérêts majeurs de la politique étrangère

La notion d'« intérêts majeurs de la politique étrangère » de la Nation n'est définie par aucune disposition constitutionnelle ou légale, de sorte que son contenu est autant indéfini que potentiellement large. En effet, le pouvoir exécutif déterminant seul sa politique étrangère, il détermine arbitrairement les objectifs couverts par cette notion.

Ainsi, en autorisant le recours aux techniques de renseignement pour la poursuite de cette finalité, le législateur a laissé le pouvoir exécutif déterminer arbitrairement les critères lui permettant de porter atteinte aux droits et libertés fondamentaux des citoyens, sans que la présente loi ne le limite en aucune façon, échouant à « prémunir les sujets de droit [...] contre le risque d'arbitraire », tel que l'exige le Conseil constitutionnel (2006-540 DC, 27 juillet 2006, cons. 9 ; 2007-557 DC, 15 novembre 2007, cons. 19 ; 2008-564 DC, 19 juin 2008, cons. 25 ; 2008-567 DC, 24 juillet 2008, cons. 39 ; 2013-685 DC, 29 décembre 2013, cons. 88).

En conclusion,

Par son expression « intérêts essentiels de la politique étrangère », le 2° de l'article 811-3 inséré au CSI par la loi déférée est entaché d'incompétence négative, le législateur ayant manqué à l'obligation que lui incombe l'article 34 de la Constitution de produire, en vue des articles 4, 5, 6 et 16 de la Déclaration de 1789, des normes intelligibles et accessibles, et doit ainsi être censuré.

Subsidiairement,

La notion d'« intérêts essentiels de la politique étrangère » peut être interprétée en tant qu'intérêt essentiel de la Nation, étant alors enfermée dans le champ limité donné par le législateur des « intérêts fondamentaux de la Nation » à l'article 410-1 du code

pénal, disposant que :

> *« Les intérêts fondamentaux de la nation s'entendent au sens du présent titre de son indépendance, de l'intégrité de son territoire, de sa sécurité, de la forme républicaine de ses institutions, des moyens de sa défense et de sa diplomatie, de la sauvegarde de sa population en France et à l'étranger, de l'équilibre de son milieu naturel et de son environnement et des éléments essentiels de son potentiel scientifique et économique et de son patrimoine culturel. »*

Au sein de cette liste, les « intérêts essentiels de la politique étrangère » correspondent précisément, pour la Nation, aux « moyens de sa défense » et de « la sauvegarde de sa population [...] à l'étranger ». Telle interprétation limiterait la possibilité du pouvoir exécutif de déterminer arbitrairement les critères lui permettant de recourir à des techniques de renseignement.

Ainsi, sous cette réserve seulement, la disposition en cause n'est pas contraire à l'objectif de valeur constitutionnelle d'intelligibilité et d'accessibilité de la loi et est conforme à la Constitution.

3.2.3. Prévention des atteintes à la forme républicaine des institutions

La notion d'« atteintes à la forme républicaine des institutions » n'est définie par aucune disposition constitutionnelle ou légale, tout au plus en est-il fait mention à l'article 410-1 du code pénal en tant qu'intérêt fondamental de la Nation, sans y être davantage définie.

Pas davantage ne sont définies les notions de « forme républicaine » ou de « République » dans la Constitution, ni la nature des « institutions » visées.

Dès lors, la définition de la notion de « forme républicaine des institutions » est laissée dans son ensemble au Gouvernement, de même que la finalité en résultant et permettant la mise en œuvre des techniques de renseignement prévues par la présente loi, sans que celle-ci ne pose aucune limite, même sémantique, quant aux objectifs concrets pouvant en être poursuivis.

En conclusion,

Le 5°, a, de l'article 811-3 inséré au code de la sécurité intérieure par la loi déférée est entaché d'incompétence négative, le législateur ayant manqué à l'obligation que lui incombe l'article 34 de la Constitution de produire, en vue des articles 4, 5, 6 et 16 de la Déclaration de 1789, des normes intelligibles et accessibles, et doit ainsi être censuré.

Subsidiairement,

La notion de « forme républicaine des institutions » peut être interprétée en ce qu'il s'agit d'un des intérêts fondamentaux de la Nation énoncés à l'article 410-1 du code pénal, introduisant le titre premier, intitulé « Des atteintes aux intérêts fondamentaux de la nation », du livre IV de ce code.

Ce titre est composé de quatre chapitres, respectivement intitulés « De la trahison et de l'espionnage », « Des autres atteintes aux institutions de la République ou à l'intégrité

du territoire national », « Des autres atteintes à la défense nationale » et « Dispositions particulières ».

Sans ambiguïté, l'intérêt fondamental de la Nation qu'est la forme républicaine des institutions est traité au deuxième de ces chapitres, traitant des « atteintes aux institutions de la République » et définissant les infractions suivantes :

*« **Article 412-1***

« Constitue un attentat le fait de commettre un ou plusieurs actes de violence de nature à mettre en péril les institutions de la République ou à porter atteinte à l'intégrité du territoire national. [...]

*« **Article 412-2***

« Constitue un complot la résolution arrêtée entre plusieurs personnes de commettre un attentat lorsque cette résolution est concrétisée par un ou plusieurs actes matériels. [...]

*« **Article 412-3***

« Constitue un mouvement insurrectionnel toute violence collective de nature à mettre en péril les institutions de la République ou à porter atteinte à l'intégrité du territoire national.

*« **Article 412-4***

« Est puni de quinze ans de détention criminelle et de 225 000 euros d'amende le fait de participer à un mouvement insurrectionnel :

« 1° En édifiant des barricades, des retranchements ou en faisant tous travaux ayant pour objet d'empêcher ou d'entraver l'action de la force publique ;

« 2° En occupant à force ouverte ou par ruse ou en détruisant tout édifice ou installation ;

« 3° En assurant le transport, la subsistance ou les communications des insurgés ;

« 4° En provoquant à des rassemblements d'insurgés, par quelque moyen que ce soit ;

« 5° En étant, soi-même, porteur d'une arme ;

« 6° En se substituant à une autorité légale.

*« **Article 412-5***

« Est puni de vingt ans de détention criminelle et de 300 000 euros d'amende le fait de participer à un mouvement insurrectionnel :

« 1° En s'emparant d'armes, de munitions, de substances explosives ou dangereuses ou de matériels de toute espèce soit à l'aide de violences ou de menaces, soit par le pillage, soit en désarmant la force publique ;

« 2° En procurant aux insurgés des armes, des munitions ou des substances explosives ou dangereuses.

*« **Article 412-6***

« Le fait de diriger ou d'organiser un mouvement insurrectionnel est puni de la détention criminelle à perpétuité et de 750 000 euros d'amende.

*« **Article 412-7***

« Est puni de trente ans de détention criminelle et de 450 000 euros d'amende le fait :

« 1° Sans droit ou sans autorisation, de prendre un commandement militaire quelconque ou de le retenir contre l'ordre des autorités légales ;

« 2° De lever des forces armées, sans ordre ou sans autorisation des autorités légales.

*« **Article 412-8***

« Le fait de provoquer à s'armer contre l'autorité de l'Etat ou contre une partie de la population est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.

« Lorsque la provocation est suivie d'effet, les peines sont portées à trente ans de détention criminelle et à 450 000 euros d'amende.

« Lorsque la provocation est commise par la voie de la presse écrite ou audiovisuelle, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables. »

Interpréter la notion d'« atteintes à la forme républicaine des institutions » comme se référant limitativement à la liste de ces infractions semble à même de rendre la finalité étudiée intelligible et accessible. Sous cette réserve seulement, la disposition en cause n'est pas contraire à l'objectif de valeur constitutionnelle d'intelligibilité et d'accessibilité de la loi et est conforme à la Constitution.

4. Services autorisés à mettre en œuvre les techniques

Le législateur a laissé le pouvoir exécutif définir sans limite le nombre de services et d'agents pouvant mettre en œuvre les techniques qu'il a autorisées, manquant à l'obligation que lui imposait la Constitution de prévoir des garanties adéquates à l'ingérence dans les droits et libertés dont il a permis l'atteinte.

En droit,

Le Conseil constitutionnel exige du législateur, en vertu de l'article 34 de la Constitution, qu'il fixe « 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, n° 2004-492 DC du 02 mars 2004, cons. 75 et 76).

En l'espèce,

L'article L. 811-3 CSI créé par la présente loi dispose que « Pour le seul exercice de leurs missions respectives, les services spécialisés de renseignement peuvent recourir aux techniques mentionnées au titre V du présent livre pour le recueil des renseignements relatifs à la défense et à la promotion des intérêts fondamentaux de la Nation » définis au présent article.

L'article L. 811-2 dispose alors que « les services spécialisés de renseignement sont désignés par décret en Conseil d'État. »

Enfin, l'article L.811-4 prévoit que :

> *« Un décret en Conseil d'État, pris après avis de la Commission nationale de contrôle des techniques de renseignement, désigne les services, autres que les services spécialisés de renseignement, relevant des ministres de la défense et de l'intérieur ainsi que des ministres chargés de l'économie, du budget ou des douanes, qui peuvent être autorisés à recourir aux techniques mentionnées au titre V du présent livre dans les conditions prévues au même livre. Il précise, pour chaque service, les finalités mentionnées à l'article L. 811-3 et les techniques qui peuvent donner lieu à autorisation. »*

Premièrement, la présente loi autorise les services visés aux articles L. 811-2 et L. 811-4 à mettre en œuvre l'ensemble des techniques de renseignement qu'elle prévoit et qui

portent manifestement atteinte au droit au respect de la vie privée de l'ensemble de la population. Il revenait donc au législateur de fixer les garanties fondamentales nécessaires afin d'assurer la juste conciliation entre ces atteintes et les finalités invoquées.

Secondement, les techniques autorisées seront directement mises en œuvre par les agents des services visés, et la totalité des renseignements collectés sera directement traitée dans leurs mains. Or, compte tenu tant de la technicité de ces mesures que de la masse d'informations qu'elles permettent de collecter sur de nombreux citoyens, elles comportent par substance un risque d'abus, de dévoiement ou de simple dysfonctionnement.

Dès lors, l'ampleur d'un tel risque pour les libertés dépend directement, d'une part, du nombre d'agents et services mettant en œuvre ces techniques et, d'autre part, de l'efficacité du contrôle pouvant être fait de l'activité de ces agents par une autorité indépendante. Toutefois, concrètement, l'efficacité de ce contrôle dépend aussi du nombre d'agents et de services contrôlés par cette autorité.

Ainsi, le risque que les techniques autorisées par la présente loi soient mises en œuvre en violation de celle-ci est proportionnel au nombre d'agents et de services pouvant les réaliser et, partant, la limitation de ce nombre était une garantie fondamentale au respect des droits en cause que le législateur aurait dû prendre et n'a pas prise.

De plus, l'effectivité des garanties qu'aurait par ailleurs prévues le législateur dans la présente loi ne saurait aussi être appréciée qu'au regard de ce nombre. Or, en laissant le pouvoir exécutif fixer ce nombre librement, le législateur a permis à ce dernier de moduler l'effectivité des garanties encadrant sa propre action en désignant un nombre plus ou moins important d'agents et de services.

Les effets de ce défaut de limitation du nombre de services pouvant être autorisé par simple décret à mettre en œuvre ces techniques sont d'autant plus importants de ce que l'article L. 811-4 y inclut « les services, **autres que les services spécialisés de renseignement**, relevant des ministres de la défense et de l'intérieur ainsi que des ministres chargés de l'économie, du budget ou des douanes ». Les risques d'abus et de dysfonctionnement, ainsi que la difficulté pratique du contrôle, sont en effet d'autant plus importants que les services concernés ne sont pas spécialisés et ont recours aux techniques de renseignement dans le cadre d'une activité bien plus large que la seule mise en œuvre de ces techniques et poursuivant des intérêts bien plus divers que les seuls intérêts fondamentaux de la Nation visés à l'article L. 811-3 du CSI.

En conclusion,

La loi déférée est entachée d'incompétence négative, le législateur ayant manqué à l'obligation que lui incombe l'article 34 de la Constitution d'assurer, en vue de l'article 2 de la Déclaration de 1789, la juste conciliation entre les intérêts qu'il défend et le respect des droits et libertés fondamentaux des citoyens, en ne limitant pas le nombre d'agents et de services pouvant porter atteinte aux droits et libertés protégés, et doit ainsi être censurée.

Au moins, l'article L. 811-4 créé par la loi déférée doit être censuré, le législateur ayant échoué à prévoir les garanties que la Constitution lui imposait de prendre en permettant à des services non spécialisés de recourir à des techniques de surveillance.

5. Notion d'« informations ou documents »

L'article 5 de la présente loi crée un titre V intitulé « *Des techniques de recueil de renseignement soumises à autorisation* », chapitre Ier « *Des accès administratifs aux données de connexion* », qui contient notamment les dispositions suivantes :

> « ***Article L. 851-1.*** *(ancien article L. 246-1)*
> « *Dans les conditions prévues au chapitre Ier du titre II du présent livre*[1]*, peut être autorisé le recueil, auprès des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, des* ***informations ou documents*** *traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications. [...] »*
>
> « ***Article L. 851-2.*** *— I. — Dans les conditions prévues au chapitre Ier du titre II du présent livre et pour les seuls besoins de la prévention du terrorisme, peut être individuellement autorisé le recueil en temps réel, sur les réseaux des opérateurs et des personnes mentionnés à l'article L. 851-1, des* ***informations ou documents*** *mentionnés au même article L. 851-1 relatifs à une personne préalablement identifiée comme présentant une menace. [...] »*
>
> « ***Article L. 851-3.*** *— I. — Dans les conditions prévues au chapitre Ier du titre II du présent livre et pour les seuls besoins de la prévention du terrorisme, il peut être imposé aux opérateurs et personnes mentionnés à l'article L. 851-1 la mise en œuvre sur leurs réseaux de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste.*
> « *Ces traitements automatisés utilisent exclusivement les* ***informations ou documents*** *mentionnés à l'article L. 851-1, sans recueillir d'autres données que celles qui répondent à leurs paramètres de conception et sans permettre l'identification des personnes auxquelles les informations ou documents se rapportent. [...] »*

En résumé, l'article L. 851-1 (ancien article L. 246-1, modifié) vise « des informations ou documents **traités *ou* conservés** par [les] réseaux ou services de communications

1. Remplace : « Pour les finalités énumérées à l'article L. 241-2 ».

électroniques » des opérateurs de communications électroniques, d'une part, et des fournisseurs d'accès à Internet et des hébergeurs, d'autre part (les personnes respectivement mentionnées à l'article L. 34-1 du code des postes et des communications électroniques et aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique).

Ces « informations ou documents » peuvent être collectés par la mise en œuvre de multiples techniques de recueil de renseignement, à savoir les techniques décrites aux articles L. 851-1, L. 851-2 et L. 851-3 tels qu'ils résultent de la présente loi (pour l'analyse consacrée aux articles L. 851-2 et -3, voir section 7 page 53).

Or, d'une part, la formule choisie par le législateur pour désigner ces « informations ou documents » rend inintelligibles et inaccessibles les dispositions qui s'y réfèrent (section 5.1) et, d'autre part, leur collecte porte une atteinte aux droits et libertés fondamentaux telle qu'il s'agit d'en cerner exactement la portée (section 5.2 page 39).

5.1. L'inintelligibilité des dispositions visant des « informations ou documents »

En visant l'accès à des « informations ou documents », qu'il s'abstient de définir de manière univoque, le législateur prive de garanties légales les dispositions susvisées encadrant les techniques de recueil de renseignement, au mépris des exigences constitutionnelles tirées notamment de l'article 34 de la Constitution.

À titre de remarque liminaire, le Conseil constitutionnel a été saisi d'une question prioritaire de constitutionnalité transmise par décision du Conseil d'État du 5 juin 2015 et enregistrée sous le numéro 2015-478 QPC, relative à l'article L. 246-1, modifié par la présente loi et renuméroté L. 851-1.

En droit, l'article 34 de la Constitution dispose que :

> *« La loi fixe les règles concernant :*
>
> *« – les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; la liberté, le pluralisme et l'indépendance des médias ; [...] »*

C'est donc exclusivement au législateur qu'il incombe de fixer les conditions d'application des libertés publiques dont jouissent les citoyens. Parmi ces libertés figurent le droit à la vie privée ainsi que la liberté d'expression et de communication, qu'implique le respect des droits reconnus respectivement aux articles 2 et 11 de la Déclaration de 1789.

Ainsi, le Conseil a dégagé des articles 4, 5, 6 et 16 de la Déclaration de 1789 un objectif de valeur constitutionnelle d'intelligibilité et d'accessibilité de la loi qui, avec l'obligation qu'a le législateur « *d'exercer pleinement la compétence que lui confie la Constitution et, en particulier, son article 34* », impose à ce dernier « *d'adopter des dispositions suffisamment précises et des formules non équivoques* » afin de « *prémunir les sujets de droit contre une interprétation contraire à la Constitution ou contre le risque d'arbitraire, sans reporter sur des autorités administratives ou juridictionnelles le soin de fixer des règles dont la détermination n'a été confiée par la Constitution qu'à la loi* » (Cons. const. décisions n^{os} 2006-540 DC, 27 juillet 2006, cons. 9 ; 2007-557 DC, 15 novembre 2007,

cons. 19 ; 2008-564 DC, 19 juin 2008, cons. 25 ; 2008-567 DC, 24 juillet 2008, cons. 39 ; 2013-685 DC, 29 décembre 2013, cons. 88).

À défaut, de telles dispositions devraient être censurées en sanction de l'incompétence négative du législateur.

Le Conseil a ainsi pu exiger qu'une disposition ne soit pas « *susceptible d'au moins deux interprétations* » (n° 85-191 DC du 10 juillet 1985, cons. 5), excluant toute formule qui « *risquerait de créer la confusion dans l'esprit* » des citoyens (n° 2003-475 DC du 24 juillet 2003, cons. 21 à 26).

Avant de développer en quoi le législateur a échoué à définir une notion que la Constitution lui imposait d'encadrer, il est utile de revenir sur les éléments des débats parlementaires qui la concernent, lesquels éclairent sur le caractère tout à fait équivoque de cette notion d'« informations ou documents ».

5.1.1. Le caractère équivoque de la notion d'« informations ou documents »

5.1.1.1. Les types de données susceptibles d'être concernés

5.1.1.1.1 La notion de « métadonnée » : À plusieurs moments durant les débats parlementaires, il a été fait référence à la notion de « **métadonnée** », pour décrire les informations et documents couverts par l'article L. 851-1, et par conséquent par les articles qui s'y réfèrent.

Ce terme est une traduction de "*metadata*", utilisé en anglais et en particulier par l'administration américaine dans les débats qui font suite aux révélations d'Edward Snowden sur les pratiques de la NSA.

Il s'agit en réalité d'un terme de l'informatique. En effet, dans les systèmes de gestion de fichiers informatiques, la donnée, "*data*", est le contenu d'un fichier. La métadonnée, "*metadata*", désigne alors toutes les informations à propos de la donnée, du fichier, sauf son contenu réel. On entend ainsi par métadonnées notamment le nom du fichier, le type de données qu'il contient, le nom du programme utilisé pour le créer, le nom de l'utilisateur propriétaire du fichier sur le système, les droits d'accès, les dates de sa création et de sa dernière modification et le nom de l'utilisateur associé, la date de la dernière lecture et le nom de l'utilisateur associé, etc. La liste exacte des métadonnées change d'un système informatique à l'autre.

5.1.1.1.2 Pour les communications téléphoniques : Par analogie, on entend en général dans le monde de la téléphonie par métadonnées toutes les informations portant sur une communication, à l'exception du contenu de la conversation elle-même — l'ensemble de ces informations pouvant être particulièrement large, sans qu'une définition exacte en soit donnée. De manière évidente, on s'attend à trouver l'identifiant de l'appelant (numéro de téléphone, numéro de contrat d'abonnement, informations associées au contrat), l'identifiant de l'appelé (idem), les date et heure du début de l'appel, la durée de l'appel, les date et heure de fin. De manière moins évidente, on y associe souvent des informations géographiques : position de l'appelant si l'appel se fait depuis un équipe-

ment mobile (antennes GSM couvrant l'appareil, donnant une position à quelques mètres près), accès Internet utilisé si c'est un appel de téléphonie sur Internet, ligne fixe utilisée si c'est un appel sur une ligne fixe, et les mêmes informations sur l'appelé.

Des informations bien plus inattendues sont en général associées à une communication chez les opérateurs. Par exemple, dans le cas d'un forfait pré-payé, le solde du compte au début de l'appel, les différents tickets de décrémentation de ce solde au cours de l'appel, le solde restant du compte pré-payé à la fin de l'appel. De même que des informations de tarification : ticket indiquant un changement de tarification au cours de l'appel (par exemple à l'heure du passage au tarif de nuit), ticket indiquant une tarification spéciale, informations indiquant par quels opérateurs intermédiaires l'appel est acheminé (par exemple lorsqu'un téléphone accroche la borne GSM d'un autre opérateur que celui de l'abonné dans le cadre d'un accord de partage de réseau en zone peu dense, ou en cas de roaming, à l'étranger).

Enfin, d'un point de vue strictement technique, toutes les informations connues sur l'abonné (adresse, type d'abonnement, agence où il s'est abonné, campagne marketing dans le cadre de laquelle il a été recruté, appels au support, autres offres souscrites, incidents de paiement, anciennes adresses, anciens abonnements, etc.) peuvent être considérées comme des métadonnées : ce sont des informations liées à l'appel, *via* l'identifiant de l'appelant ou de l'appelé, qui ne sont pas le contenu.

5.1.1.1.3 Pour les fournisseurs d'accès à Internet : Dans le cas d'un accès à Internet fixe, les métadonnées recouvrent un ensemble d'informations beaucoup plus limité : ligne fixe utilisée [2], début de la connexion à Internet, fin de la connexion, adresse IP attribuée lors de la connexion, quand cette adresse n'est pas fixe. Toutes les informations autour de l'abonné (contrats, adresse postale, paiements, etc.) sont les mêmes que pour le cas de la téléphonie.

Dans le cas d'un accès à Internet mobile, les informations disponibles sont en général plus nombreuses. On y retrouve au minimum des informations sur l'équipement utilisé, sa localisation géographique exacte au cours de la connexion. Par ailleurs, chez certains opérateurs, les accès au Web se font au travers de relais, dits « proxy », qui notent l'adresse exacte de chaque page visitée [3]. Dans un tel cas, l'adresse URL exacte de chaque page visitée, l'heure de la visite, y compris l'adresse exacte de chaque fragment externe de la page (publicité, bouton « like » Facebook et assimilés, contenu agrégé depuis un autre site, etc.) sont conservées — et relèvent alors manifestement du contenu de la correspondance.

5.1.1.1.4 La notion de « données de connexion » : La notion de « **données de connexion** » ne semble pas avoir non plus de définition précise en droit. Elle est cependant utilisée dans le titre du chapitre où se trouve l'article L. 851-1 tel qu'il ressort de la loi déférée, comme elle se trouvait dans le titre du chapitre où se trouvait l'ancien

2. À noter que le câble n'offre pas cette information, mais seulement le quartier de raccordement, mais qu'en revanche la technologie utilisée permet d'avoir un identifiant de l'appareil utilisé pour se connecter, le modem ou la « box ».

3. C'est par exemple la seule technique possible pour que le trafic vers un site donné ne soit pas décompté du forfait mensuel ou du *fair use* lié à certains abonnements.

article L. 246-1 du CSI. On la retrouve également à l'article L. 854-1-II [4].

On peut supposer, sans que ce soit clairement établi, que cette notion recouvre les données conservées par les opérateurs, hébergeurs et éditeurs de services au titre de l'article 6 de la Loi pour la confiance dans l'économie numérique du 21 juin 2004 (LCEN) et/ou de l'article L. 34-1 du code des postes et communications électroniques (CPCE). Ces deux articles posant des difficultés d'interprétation comme il sera vu *infra*.

5.1.1.2. Le sens retenu lors des débats parlementaires

Le débat au Sénat a permis d'apporter un éclairage, faible, sur les intentions des rédacteurs du texte sur ce sujet. En effet, l'amendement numéro 155 rectifié, proposait :

> *« Alinéa 8*
>
> *« Remplacer les mots : "les informations ou documents" par les mots : "les données de connexion". »*

L'amendement sera rejeté après un avis défavorable de la commission et du gouvernement, formulé en ces termes [5] :

> **M. le président.** Quel est l'avis de la commission ?
>
> **M. Philippe Bas**, *rapporteur*. La commission émet un avis défavorable, monsieur le président.
>
> Sans entrer dans des détails inutiles, j'indique que la technique de renseignement évoquée permet de recueillir non seulement des données de connexion, mais également d'autres éléments couverts par l'expression « informations ou documents ». Vouloir restreindre le champ d'application de l'alinéa 8 de l'article 2 au recueil des données de connexion me semble être une erreur. Il faut conserver les termes « les informations ou documents », car ils recouvrent notamment les données techniques permettant l'identification des numéros d'abonnement, les fadettes et les données relatives à la localisation des équipements, **et pas seulement les données de connexion**.
>
> **M. le président.** Quel est l'avis du Gouvernement ?
>
> **M. Jean-Yves Le Drian**, *ministre*. Le Gouvernement est défavorable à cet amendement, non pas tant sur le fond, quoique la notion de « documents » permette de viser notamment les factures que les abonnés remettent à leurs opérateurs lors de l'ouverture de leur compte et qui peuvent faire partie des documents sollicités par les services, que sur la forme. En effet, depuis 1991, **l'expression « informations et documents »** est utilisée pour qualifier les données de connexion. Elle figure ainsi à l'article 20 de la loi de programmation militaire de 2006. D'ailleurs, elle **ne suscite plus d'ambiguïté aujourd'hui et renvoie à des données précisément *définies dans des textes réglementaires***.
>
> Dans ces conditions, il semble préférable de maintenir cette expression, par cohérence avec les autres textes où elle est employée.

4. « (...)Les *données de connexion* associées à ces correspondances sont conservées et détruites dans les conditions prévues aux mêmes articles L. 822-2 à L. 822-4 ».

5. Texte repris du compte rendu intégral des débats tel que diffusé par le site Web du Sénat à l'adresse `http://www.senat.fr/seances/s201506/s20150603/s20150603014.html#amd_2014_461_155_rect_1`

Rappelons d'emblée que, contrairement à ce que considère le ministre, le sens de l'expression « informations et documents » dans le code de la sécurité intérieure n'est pas dépourvu d'ambiguïté, dans la mesure où elle fait l'objet d'une question prioritaire de constitutionnalité transmise par le Conseil d'État le 5 juin 2015 (QPC n° 2015-478).

La lecture des débats au Sénat montre en réalité le caractère extrêmement équivoque de la notion. La volonté des parlementaires, qui se rangent aux avis exprimés par le rapporteur et par le Gouvernement, devient alors explicite : la formule « informations et documents » vise explicitement « *non seulement des données de connexion, mais également d'autres éléments* » selon le rapporteur, qui précise bien que la formule ne couvre « *pas seulement les données de connexion* », et le ministre de se défausser en prétextant que la formule « *renvoie à des données précisément définies dans des textes réglementaires* ».

Ainsi, il apparaît que le gouvernement et le législateur sont en réalité incapables de fournir une définition précise, ni une liste exhaustive des catégories de données correspondant à la notion « informations ou documents ». Ce faisant, le législateur a entièrement abandonné son obligation de limiter le champ des dispositions concernées, laissant ce rôle au pouvoir réglementaire.

5.1.2. L'absence de définition législative des « informations ou documents » concernés

Au regard de son caractère équivoque, l'inintelligibilité et l'inaccessibilité de la formule choisie par le législateur sont manifestes à deux titres : premièrement, le législateur en renvoie au pouvoir réglementaire la définition alors que la Constitution la lui attribuait ; secondement, le législateur l'emploie par référence à d'autres dispositions légales elles-mêmes inintelligibles.

5.1.2.1. Le renoncement du législateur à définir clairement la notion d'« informations ou documents »

Comme démontré à la section 5.1.1 page 33, la nature technique des « informations ou documents » visés à l'article L. 851-1 du CSI est particulièrement équivoque, le législateur ayant explicitement refusé, à la vue des débats parlementaires, de délimiter cette notion par des critères objectifs, en suivant l'avis du Gouvernement lorsque son ministre, prétextant que « *l'expression « informations et documents » [...] ne suscite plus d'ambiguïté aujourd'hui et renvoie à des données précisément définies dans des textes réglementaires* », l'invitait à laisser au pouvoir réglementaire le soin de définir cette notion.

En effet, les « informations ou documents » visés à l'ancien article L. 246-1 du CSI, repris par l'article L. 851-1, sont définis par le pouvoir réglementaire à l'article R. 246-1 du même code, par renvoi aux « articles R. 10-13 et R. 10-14 du code des postes et des communications électroniques et à l'article 1er du décret n° 2011-219 du 25 février 2011 » qui définissent respectivement les informations que les opérateurs doivent et peuvent conserver au titre de l'article L. 34-1 du CPCE et celles que les fournisseurs d'accès à Internet et les hébergeurs doivent conserver au titre de l'article 6, II, de la loi du 21 juin 2004 pour la confiance dans l'économie numérique.

Il en ressort notamment que, au regard des explications faites *supra* sur la notion de « méta-données » (partie 5.1.1.1 page 33), le législateur a laissé au pouvoir réglementaire le choix de déterminer si les services de renseignement peuvent recueillir auprès de certains fournisseurs d'accès à Internet la liste des pages Web consultées par leurs clients, alors que l'équilibre de l'ensemble de la présente loi dépend pour une part importante de ce choix.

En conclusion,

Les articles L. 851-1, L. 851-2 et L. 851-3 insérés au CSI par la présente loi sont entachés d'incompétence négative, le législateur ayant manqué, en déterminant leur champ par référence à la seule notion d'« informations ou documents », à l'obligation que lui incombe l'article 34 de la Constitution de produire, en vue des articles 4, 5, 6 et 16 de la Déclaration de 1789, des normes intelligibles et accessibles, et doivent ainsi être censurés.

5.1.2.2. L'inintelligibilité des dispositions visant les personnes traitant les « informations ou documents »

L'article L. 851-1 créé par la loi déférée vise « des informations ou documents » qui sont *traités ou conservés* par les *réseaux ou services* de communications électroniques des :

1. opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ;
2. des personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi n° 2004-575.

Cependant, en renvoyant à ces dispositions, le législateur échoue à définir de façon univoque les personnes traitant ou conservant les informations ou documents concernés, ces dispositions étant elles-mêmes inintelligibles. En effet, bien que les personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 visent respectivement et sans équivoque les *fournisseurs d'accès à Internet* et les *hébergeurs de site Web*, à l'inverse, l'article L. 34-1 s'appuie quant à lui sur la notion d'« *opérateurs de communications électroniques* », laquelle est extrêmement vague. En effet, cette notion renvoie à l'article L. 32 du CPCE, qui la présente ainsi :

> *« **1° Communications électroniques.***
>
> *« On entend par communications électroniques les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique.*
>
> *« **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.

[...]

« 6º Services de communications électroniques.

« On entend par services de communications électroniques les prestations consistant entièrement ou principalement en la fourniture de communications électroniques. Ne sont pas visés les services consistant à éditer ou à distribuer des services de communication au public par voie électronique.

[...]

« 15º Opérateur.

« On entend par opérateur toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques.

Or, plusieurs interprétations se confrontent quant à la question de savoir si les prestataires qui fournissent des services de correspondance électronique (messagerie électronique, discussion interactive écrite, audio ou vidéo, messagerie interne aux réseaux sociaux ou aux entreprises, etc.) sont concernés comme « opérateurs » au sens de l'article L. 34-1 du CPCE et, dès lors, si les « informations et documents » qu'ils traitent et conservent par leurs services — et qui concernent la correspondance électronique de l'ensemble de la population — peuvent être recueillis par les services de renseignement. Or, aucune réponse à cette question n'est acquise à présent ; des pratiques coexistent selon l'interprétation faite par les autorités publiques de la notion d'opérateur.

La première interprétation, qui semble être celle retenue par l'Autorité de régulation des communications électroniques et des postes (ARCEP), est que les prestataires de services de correspondances en ligne ne sont pas des opérateurs. En témoigne le registre des opérateurs de communications électroniques tenu par l'ARCEP [6].

La seconde interprétation, qui semble être celle retenue par les services de police judiciaire et par les services de police administrative, est que ces prestataires sont des opérateurs. C'est par exemple sur cette base que les services demandent déjà aux fournisseurs de services de messagerie les données sur les courriers reçus ou envoyés depuis une adresse de messagerie électronique.

Dès lors, la limitation des données pouvant être collectées sur l'ensemble de la population dépend en grande partie de l'interprétation retenue de la notion d'opérateur, déterminant si y sont comprises ou non les données concernant les correspondances émises par voies électroniques.

L'incertitude quant à cette interprétation étant par ailleurs exacerbée par les pratiques des administrations, il apparaît que le législateur a renvoyé à une disposition « *susceptible d'au moins deux interprétations* » [7] le très faible encadrement des atteintes aux droits et libertés fondamentaux qu'il autorise, privant ainsi l'ensemble des citoyens de pouvoir en « *mesurer utilement la portée* » [8] et violant dès lors le principe d'intelligibilité et d'accessibilité de la loi imposé par la Constitution.

6. ARCEP, La liste des opérateurs déclarés, disponible en ligne `https://extranet.arcep.fr/portail/LinkClick.aspx?fileticket=Dh7Vr2GF5vw%3d&tabid=215&portalid=0&mid=720`

7. Cons. const., décision 85-191 DC, 10 juillet 1985, cons. 5

8. Cons. const., décision 2005-530 DC, 29 décembre 2005, cons. 77

En conclusion,

La référence faite aux « opérateurs de communications électroniques et [aux] personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques » au nouvel article L. 851-1 du CSI est entachée d'incompétence négative, le législateur ayant manqué, en l'employant, à l'obligation que lui incombe l'article 34 de la Constitution de produire, en vue des articles 4, 5, 6 et 16 de la Déclaration de 1789, des normes intelligibles et accessibles, et doit ainsi être censurée.

5.2. L'importance des atteintes portées aux droits au respect de la vie privée et à la liberté de communication

Si toutefois la notion d'« informations ou documents » avait été précisément définie par le législateur pour ne viser exclusivement que des données de connexion ou des métadonnées précises suivant une définition clairement délimitée, l'accès à de telles données permis par l'article L. 851-1 de la loi déférée porterait tout de même une atteinte considérable aux droits et libertés garantis par la Constitution.

Un exposé s'impose pour comprendre en quoi l'accès aux données de connexion ou métadonnées n'est pas, en soi, moins attentatoire aux droits et libertés garantis par la Constitution que l'accès aux contenus des correspondances.

En effet, l'ingérence dans la vie privée des individus représentée par l'accès aux métadonnées est souvent considérée, **à tort**, comme étant moins grave que celle représentée par l'accès au contenu des correspondances. Les raisons de l'abolition de cette différence sont liées à la fois à la l'évolution de la technologie et des usages, mais aussi à l'évolution des techniques de collecte et d'analyse des renseignements recueillis.

5.2.1. Dans le traitement manuel

À supposer une collecte manuelle, pour ainsi dire *artisanale*, des données, par laquelle un être humain traite et analyse la totalité des données collectées, comme ce fut le cas en matière d'interception téléphonique jusqu'à la fin du siècle dernier : un individu est placé sur écoute, ses conversations sont toutes enregistrées sur bandes, des agents retranscrivent la totalité de ces bandes, et produisent des synthèses de ces conversations. Dans ce cas de figure, la donnée produite est riche, parce qu'elle est qualifiée, alors que la métadonnée (Monsieur X a téléphoné à Madame Y à 22h37, l'appel a duré 3 minutes et 18 secondes, il a été facturé en heures creuses) est relativement pauvre.

Dans certains cas de figure, néanmoins, ces informations peuvent devenir de véritables renseignements à travers une analyse statistique des métadonnées, ce qui est relativement difficile à réaliser dans le cas d'un traitement manuel : par exemple, mesurer que la personne surveillée a des contacts de plus en plus divers, ou au contraire de moins en moins divers, révèle une variation qui est un indicateur relativement fiable d'un changement dans son mode de vie.

5.2.2. Dans les traitements automatiques

L'analyse automatique des données — des contenus — est, le plus souvent, périlleuse voire aléatoire. Dans le cas des échanges téléphoniques, il faut commencer par supposer que le logiciel de reconnaissance vocale sera capable de faire une transcription fiable d'un locuteur qui ne fait aucun effort pour être compris de la machine. Mais, même en supposant que l'échange soit déjà un texte écrit (textos, courriers électroniques, etc.), l'analyse automatique pour extirper une information structurée est complexe : il faut comprendre les allusions, les sous-entendus, le second degré, les non-dits implicites d'une conversation à l'autre, etc.

À l'exact opposé, les métadonnées disent presque tout sur l'individu, et sont d'une analyse automatique beaucoup plus simple, parce qu'elles sont déjà *structurées*. Deux personnes, qui ne communiquaient pas ensemble, ou très peu, se mettent à échanger des dizaines de messages, tous les jours, par exemple. Quel que soit le contenu de leurs échanges, il s'agit d'un signe fort qu'une relation vient de se créer. Il pourrait être plus délicat de déterminer si cette relation est intime ou non. Mais les données de géolocalisation des téléphones mobiles peuvent être très explicites : présence simultanée, dans un même lieu, des deux individus, heures de présence, durée de la rencontre — tout y est.

Au final, les métadonnées disent des choses plus claires et plus facilement analysables par un ordinateur que les données elles-mêmes. La taille des messages, les heures d'envoi, leur fréquence, disent plus de choses que « On dîne ce soir ? » ou « Je serai en retard ».

5.2.3. Différences entre intermédiaires techniques

Les métadonnées peuvent être collectées auprès de deux sortes d'acteurs de l'environnement des communications électroniques, à savoir l'opérateur de communications électroniques (dont les fournisseurs d'accès à Internet, de téléphone, mail, texto, tchat, etc.), l'hébergeur de site web, mais aussi d'autres services de la société de l'information qui sont moins directement liés aux activités de surveillance.

5.2.3.1. Opérateurs de communications électroniques

La métadonnée la plus pauvre est celle fournie par le fournisseur d'accès à Internet : Monsieur X a redémarré sa *box* le 12 avril à 22h35, elle est restée allumée jusqu'au 15 mai à 15h30. Au mieux, une information plus fine, mais équivalente : il a eu l'adresse IP numéro x le 12 avril de 12h35 à 23h55, puis l'adresse y jusqu'au 13 avril à 19h27, etc. Les seules informations pertinentes qui puissent être tirées de ces informations sont faibles : l'individu laisse sa *box* allumée ou pas, les heures auxquelles il l'allume.

Si la notion « informations ou documents » est interprétée de sorte à permettre le recueil auprès des fournisseurs d'accès d'informations sur les volumes de données échangées (beaucoup de trafic Internet à telle heure, peu de trafic à tel autre moment, etc.), il devient possible de savoir s'il est plutôt consommateur de vidéos ou de textes, et à quelles heures il utilise le réseau.

La métadonnée fournie par l'opérateur de communication électronique, c'est-à-dire par le fournisseur du service (téléphonie mobile, courrier électronique, messagerie instantanée,

etc.) est la plus riche. Elle dit exactement quand, à quel endroit, à quelle fréquence, et avec qui chacun échange. Le type même de la messagerie retenue donne des informations très fines : la messagerie d'un site de rencontre n'a pas les mêmes usages que le texto habituel ou qu'une messagerie « généraliste » comme Skype.

5.2.3.2. Hébergeurs

La métadonnée fournie par l'hébergeur de site web ne donne pas vraiment des informations sur un individu *a priori*, elle donne en fait des informations sur tous les individus en lien avec le site web : qui s'y connecte, est-ce en mode lecture ou en mode écriture, qui a laissé des commentaires, quand, etc. Cette information permet par exemple de dresser des statistiques très fines sur le lectorat d'un site de presse, ou sur la fréquentation d'un site politique. Elle ne révèle des informations sur un individu donné que si on sait *à l'avance* que l'individu fréquente le site à un titre ou à un autre.

5.2.3.3. Autres services de la société de l'information

Tous les autres services de la société de l'information tendent à produire des données, et des métadonnées. À chaque fois que ces (méta)données peuvent être reliées à un individu, elles donnent des informations sur lui. Si on suppose par exemple une application permettant de faire un suivi de régime, les données sont les calories consommées chaque jour, sous quelle forme, etc. La métadonnée indique la période pendant laquelle l'application a été utilisée, depuis quels équipements (téléphones, tablettes, ordinateurs, etc.), dans quels lieux, etc.

5.2.4. Accès aux données ou aux contenus : une atteinte aux droits d'une gravité équivalente

Par une décision du 19 janvier 2006 portant sur les accès administratifs aux données de connexion, le Conseil constitutionnel a considéré que l'accès à des données techniques représentait une ingérence relativement limitée dans la vie privée des personnes.

> *« 8. Considérant, en premier lieu, que l'article 66 de la Constitution, aux termes duquel : « Nul ne peut être arbitrairement détenu. - L'autorité judiciaire, gardienne de la liberté individuelle, assure le respect de ce principe dans les conditions prévues par la loi », ne saurait être méconnu par une disposition* ***qui se borne à instaurer une procédure de réquisition de données techniques*** *;*
>
> *« 9. Considérant, en deuxième lieu, qu'il appartient au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public, nécessaire à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des libertés constitutionnellement garanties, au nombre desquelles figurent le respect de la vie privée et la liberté d'entreprendre, respectivement protégés par les articles 2 et 4 de la Déclaration des droits de l'homme et du citoyen de 1789 ;*
>
> *« 10. Considérant, en l'espèce, que le législateur a assorti la procédure de réquisition de données techniques qu'il a instituée de limitations et précautions, précisées ci-dessus, propres à assurer la conciliation qui lui incombe entre, d'une part, le respect de la vie*

privée des personnes et la liberté d'entreprendre des opérateurs, et, d'autre part, la prévention des actes terroristes, à laquelle concourt ladite procédure ; »

(Déc. 2005-532 DC du 19 janvier 2006, cons. 8 à 10)

Cette décision reflète cependant un état de fait qui précède la forte augmentation de l'utilisation des communications électroniques *via* des appareils mobiles. Les données techniques sont désormais porteuses d'informations plus exhaustives et plus intrusives.

Cette décision reflète également un état du droit qui, depuis, a évolué. Le nombre et l'étendue des finalités pour lesquelles l'accès aux données est autorisé ainsi que le nombre de services pouvant en faire la réquisition ayant augmenté.

L'équilibre entre le respect de la vie privée d'une part, et les finalités pour lesquelles l'accès aux données de connexion est autorisé d'autre part, a indubitablement changé.

Dans ses conclusions relatives à la transmission de la question prioritaire de constitutionnalité dans l'affaire n° 2015-478 QPC, le rapporteur public près le Conseil d'État expose que le changement des modes d'utilisation des communications électroniques se traduit par « *une amélioration de la précision des informations* ». Selon lui, la situation est même telle que « *la summa divisio entre accès de données et accès de contenus n'a probablement plus la même portée qu'il y a quelques années, et* ***sans doute l'ingérence dans la vie privée que constitue l'accès aux données de connexion doit être réévalué*** » [9].

Par ailleurs, la Grande chambre de la CJUE a clairement pris acte de cet état de fait et en tire les conséquences de droit dans son arrêt *Digital Rights* du 8 avril 2014 :

*« **27.** [Les données de connexion] sont susceptibles de **permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées**, 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.*

[...]

***56.** Quant à la question de savoir si l'ingérence que comporte la directive 2006/24 est limitée au strict nécessaire, il convient de relever que cette directive impose, conformément à son article 3 lu en combinaison avec son article 5, paragraphe 1, la conservation de toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès à l'internet, le courrier électronique par Internet ainsi que la téléphonie par l'internet. Ainsi, elle vise tous les moyens de communication électronique dont l'utilisation est très répandue et d'une importance croissante dans la vie quotidienne de chacun. En outre, conformément à son article 3, ladite directive couvre tous les abonnés et utilisateurs inscrits. Elle comporte donc une ingérence dans les droits fondamentaux de la quasi-totalité de la population européenne.*

[...]

*« **65.** Il résulte de ce qui précède que la directive 2006/24 ne prévoit pas de règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte. **Force est donc de constater que cette directive comporte une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle***

9. Propos retranscrits et cités dans `http://www.nextinpact.com/news/95334-donnees-connexion-qpc-quadrature-fdn-et-ffdn-transmise-au-conseil-constitutionnel.htm`.

ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire. »

(CJUE, *Digital Rights Ireland*, C-293/12, Grande chambre, 8 avril 2014)

De même, dans ses conclusions sur cette affaire [10], l'avocat général Pedro Cruz Villalón soulignait quant à lui que, même si « *la directive 2006/24 exclut de son champ d'application, de manière aussi expresse qu'insistante, le contenu des communications téléphoniques ou électroniques, les informations communiquées elles-mêmes* », il n'en demeure pas moins qu'un tel dispositif « *constitue une* ***ingérence particulièrement caractérisée*** *dans le droit au respect de la vie privée* » (§ 70-71). Or, pour l'avocat général :

« Les effets de cette ingérence se trouvent démultipliés par l'importance acquise par les moyens de communications électroniques dans les sociétés modernes, qu'il s'agisse des réseaux mobiles numériques ou d'Internet, et leur utilisation massive et intensive par une fraction très importante des citoyens européens dans tous les champs de leurs activités privées ou professionnelles.

Les données en question, il importe également d'insister encore une fois à cet égard, ne sont pas des données personnelles au sens classique du terme, se rapportant à des informations ponctuelles sur l'identité des personnes, mais des données personnelles pour ainsi dire qualifiées, dont l'exploitation peut permettre l'établissement d'une cartographie aussi fidèle qu'exhaustive d'une fraction importante des comportements d'une personne relevant strictement de sa vie privée, voire d'un portrait complet et précis de son identité privée ».

(Conclusions de l'avocat général dans l'affaire Digital Rights*, présentées le 12 décembre 2013, § 73-74).*

Si la conservation des données de connexion permet de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, *a fortiori* l'accès à de telles données constitue également une ingérence « d'une vaste ampleur et d'une gravité particulière » au droit à la vie privée et à la liberté de communication.

Enfin, le Conseil constitutionnel a lui-même déjà souligné l'évolution majeure des moyens de communications modernes pour constater l'importance de l'atteinte à une liberté ou un droit protégé par la Déclaration de 1789 :

« Considérant qu'aux termes de l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 : « La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme : tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi » ; ***qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions****, ce droit implique la liberté d'accéder à ces services ; »*

(Décision n° 2009-580 DC du 10 juin 2009, cons. 12)

Ainsi, sa décision de 2006 sur l'accès aux métadonnées reflète une réalité technique largement dépassée. Cet état de fait est donc certainement à réévaluer à la lumière des évolutions dans l'utilisation des outils de communication électronique, et donc de la gravité nouvelle de l'atteinte à la vie privée que constitue un accès aux métadonnées.

10. Conclusions de l'avocat général dans l'affaire *Digital Rights*, présentées le 12 décembre 2013.

En conclusion,

La collecte des métadonnées constitue à tout le moins une ingérance dans le droit au respect de la vie privée aussi grande que l'interception des communications téléphoniques ou Internet. Par conséquent, elle doit être entourée des mêmes garanties légales et répondre aux mêmes exigences constitutionnelles.

Or, comme exposé *infra* (au chapitre 10 page 85), en édictant les dispositions en cause qui doivent concilier cette ingérence d'une grande ampleur dans la vie privée avec les objectifs et finalités fixés, le législateur n'a pas assuré un équilibre qui satisfasse aux exigences constitutionnelles de garanties et de contrôle.

Troisième partie

TECHNIQUES DE SURVEILLANCE

6. Analyse des communications chiffrées

À plusieurs reprises lors des débats parlementaires, tant en commission qu'en séance, le chiffrement des communications a été pointé comme étant soit une circonstance aggravante, soit le signe d'un comportement suspect.

Pourtant, la pratique de chiffrer ses communications relève à double titre de l'article 2 de la Déclaration de 1789, dont la protection implique le respect de la vie privée ainsi que la résistance à l'oppression. En effet, les techniques de chiffrement ont principalement pour objet de protéger efficacement un contenu — typiquement, un contenu qui relève de la vie privée — contre un accès non autorisé et suprebtice audit contenu.

Un exposé sur ces techniques, et les cas d'usage, est nécessaire pour comprendre les dangers posés par les dispositions de la loi déférée relatives aux données chiffrées pour les droits et libertés constitutionnellement garantis.

6.1. Éléments techniques sur le chiffrement

Deux types de méthodes de chiffrement existent : le chiffrement symétrique, et le chiffrement asymétrique :

- Le chiffrement symétrique utilise une clef pour chiffrer qui est la même pour déchiffrer, par exemple un simple mot de passe. Cette technique est en général utilisée pour chiffrer les données de l'utilisateur, par exemple pour chiffrer le disque dur de son ordinateur pour qu'en cas de vol de l'ordinateur les données ne soient pas mises en danger.
- Le chiffrement asymétrique se fait avec deux clefs, l'une sert à chiffrer, l'autre sert à déchiffrer. La clef qui sert à chiffrer est en général publique. Les deux clefs forment une paire : ce que la clef de chiffrement a chiffré ne peut être déchiffré qu'avec la clef de déchiffrement associée.

Les méthodes de chiffrement habituelles des données pour les communications sont des chiffrements asymétriques, qui fonctionnent *de bout en bout*, c'est-à-dire que l'émetteur chiffre les données (avec la clef du destinataire, publique, de chiffrement) de manière que seul le destinataire puisse les déchiffrer (en utilisant sa clef, secrète, de déchiffrement).

La notion de « données chiffrées » peut recouvrir des réalités différentes. Le mode de chiffrement dépend alors du moment, dans la communication, où a lieu le chiffrement : le chiffrement peut avoir lieu soit au niveau de la connexion au réseau lors du transport,

soit au niveau du logiciel utilisé (messagerie, tchat, etc.) :

- Une méthode de chiffrement liée à une méthode de transport de données, par exemple un VPN[1] : **tout le trafic entre l'ordinateur client et le point de connexion du VPN est chiffré**, et il est alors virtuellement impossible de savoir quoi que ce soit sur l'usage fait de cette connexion réseau.
- Une méthode de chiffrement liée à un protocole de communication, par exemple pour chiffrer les courriers électroniques, ou les textos échangés entre téléphones mobiles, **chiffre le contenu de la communication, et non les métadonnées**. Le contenu du courrier électronique se trouve ainsi uniquement lisible par son destinataire, et non pas par tous les intermédiaires participant à l'acheminement du courrier. L'analogie habituellement utilisée est de comparer les communications non chiffrées à l'utilisation de cartes postales, et les communications chiffrées à l'utilisation de courriers sous enveloppe.

Les techniques de chiffrement s'appuient sur des principes mathématiques publics et connus. Il existe des logiciels très nombreux et variés mettant en œuvre ces techniques, y compris de très nombreux logiciels libres et gratuits. Il n'y a donc aucune barrière à l'entrée de ces outils : il suffit d'utiliser ces logiciels librement disponibles, sans formation technique particulière autre que la lecture du mode d'emploi.

6.2. L'incohérence et le danger d'une logique consistant à faire du chiffrement un facteur de suspicion

Comme indiqué dans une publication récente, la méconnaissance des techniques de chiffrement peut amener à des conclusions hâtives, ou fausses :

> « La méconnaissance des réalités sociales et techniques d'Internet qui affecte certains magistrats tend en effet à renforcer certains de leurs préjugés et peut parfois laisser libre cours à quelques fantasmes de leur part. Elle les conduit à exagérer la nature et la gravité des faits reprochés et à voir dans des activités banales – par exemple le simple fait de participer à un salon de discussion IRC – un savoir-faire qui serait l'apanage d'une élite délinquante au sein du monde hacker. À l'image du juge madrilène qui, en décembre dernier, justifiait l'arrestation préventive de sept militants anarchistes en pointant leurs lectures subversives et le fait « *qu'ils utilisaient des mesures de sécurité extrêmes, telles que l'utilisation d'un serveur RISE UP* » (en fait de « *mesures de sécurité extrêmes* », le service mail de Riseup ne fait qu'appliquer les meilleures pratiques en matière de confidentialité des communications). L'inculture numérique peut ainsi conduire les juges à une répression disproportionnée en les rendant aveugles à la réalité des faits dont ils doivent juger : l'usage par des citoyens d'outils Internet « grand public » dans un but de participation démocratique.[2] »

1. *Virtual Private Network*, ou réseau privé virtuel, permet de chiffrer l'ensemble d'une connexion au réseau. Cette technologie est d'un usage très courant en entreprise pour que les personnes en mobilité aient accès au réseau interne de l'entreprise.

2. Félix Tréguer, Le droit pénal de la fraude informatique, nouvel ami des censeurs ?, *La Revue des Droits de l'Homme — Actualités Droits-Libertés*, 2 juin 2015. Disponible à l'adresse : `https://revdh.revues.org/1328`.

S'agissant du chiffrement, cette méconnaissance technique qui conduit à la suspicion est d'autant plus dommageable que, dans la pratique, les experts en sécurité informatique préconisent l'utilisation systématique de solutions de chiffrement, tant dans l'usage courant pour protéger sa vie privée, que dans les usages professionnels pour se prémunir de l'intelligence économique et du vol de données.

La même dichotomie se retrouve au sein de la puissance publique. Ainsi, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) émet régulièrement des recommandations, et œuvre sur le terrain à généraliser l'utilisation des outils de chiffrement [3].

Une plus grande utilisation des outils de chiffrement est également préconisée par différentes instances européennes. Ainsi, dans son rapport associé à la résolution 2045 du 21 avril 2015 de l'Assemblée parlementaire du Conseil de l'Europe, le député néerlandais Pieter Omzigt estime que, « en attendant que les États s'entendent sur les limites des programmes de surveillance massive de leurs services de renseignement, un cryptage généralisé destiné à renforcer le respect de la vie privée reste la riposte la plus efficace pour permettre aux citoyens de protéger leurs données » (§119) [4].

De la même manière, le rapport récent de l'unité prospective des choix techniques et scientifiques du Parlement européen appelle à la systématisation du recours au chiffrement [5]. Le résumé diffusé par le Parlement européen indique clairement [6] :

3. Ainsi par exemple, l'ANSSI maintient un référentiel général de sécurité, disponible en ligne (`http://www.ssi.gouv.fr/uploads/2015/01/RGS_v-2-0_B1.pdf`), qui indique quelles méthodes de chiffrement, et quelle taille de clef de chiffrement utiliser en fonction de la qualité de sécurité souhaitée. L'agence indique très clairement que ce sont des tailles minimales, et préconise d'utiliser systématiquement les chiffrements les plus puissants qui soient disponibles, quand c'est possible.

4. Disponible en ligne : `http://assembly.coe.int/nw/xml/Xref/Xref-XML2HTML-fr.asp?fileid=21583&lang=fr`.

5. Rapport disponible en ligne, en deux parties.
   - Stefan Schuster et al., 2015. « *Mass Surveillance : Part 1 - Risks and opporuntities raised by the current generations of network services and applications* » (PE 527.409), Parlement européen, *Science and Technology Options Assessment*, Bruxelles. Disponible à l'adresse : `http://www.europarl.europa.eu/stoa/cms/home/publications/studies?reference=EPRS_STU%282015%29527409`.
   - M. van den Berg et al., 2014. « *Mass Surveillance : Part 2 - Technology Foresight, options for longer term security and privacy improvements* » (PE 527.409), Parlement européen, *Science and Technology Options Assessment*, Bruxelles. Disponible à l'adresse : `http://www.europarl.europa.eu/stoa/cms/home/publications/studies?reference=EPRS_STU%282015%29527410`.
   - Un résumé est également disponible : `http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527410/EPRS_STU%282015%29527410%28ANN2%29_EN.pdf`.

6. Traduction par nos soins de :

> *The purpose of this policy brief is to provide the Members of the European Parliament with technology oriented policy options, regarding the protection of the European Information Society against mass surveillance. Four main themes have been identified corresponding to eleven different policy options.*
>
> ***Theme I : "Promote adoption of existing good practices"***
>
> ***1. End to End encryption (E2EE)***
>
> *Stimulate* ***awareness on the necessity of using encryption*** *by initiating a campaign, as awareness on privacy risks is fairly low. Increase the knowledge level of end-users both individuals and responsible departments in organizations (public and private), by setting up an independent platform where users can find information on tools, implementation, do's and don'ts et cetera.*

Les passages en gras le sont dans la version d'origine diffusée par le Parlement Européen.

« L'objectif de cette synthèse est de fournir aux députés européens des préconisations d'un point de vue technique sur la protection de la société de l'information européenne contre la surveillance de masse. Quatre thèmes principaux ont été identifiés correspondant à onze préconisations.

Thème I : « Promouvoir l'adoption des meilleures pratiques »

« **1. Chiffrement de bout en bout (E2EE)**

« Stimuler **la prise de conscience sur la nécessité du recours au chiffrement** en mettant en place une campagne, la mise en danger de la vie privée étant trop méconnue. Augmenter les connaissances des utilisateurs finaux, tant les particuliers que les responsables de groupes privés ou publics, en mettant en place une plateforme indépendante qui permette aux utilisateurs de trouver des informations sur les outils, les implémentations, les choses à faire, les choses à proscrire, etc. »

À l'exact opposé, M. Bernard Bajolet, directeur général de la DGSE, indique lors des débats parlementaires [7] que ses services cherchent à détecter automatiquement l'utilisation de techniques de dissimulation des communications :

« Dans le second cas, il s'agit de détecter certaines pratiques de communication. L'objectif n'est pas de surveiller des comportements sociaux, tels que la fréquentation de telle ou telle mosquée par telle ou telle personne. Mais nous connaissons les techniques qu'emploient les djihadistes pour dissimuler leurs communications et échapper à toute surveillance : ce sont ces attitudes de clandestinité qu'il s'agit de détecter afin de prévenir des attentats, sans avoir à pratiquer une surveillance de masse. »

Or ces « techniques [...] pour dissimuler leurs communications » ne peuvent faire que référence aux techniques de chiffrement ou d'anonymisation — seuls moyens effectifs de protéger ses communications en ligne. Dès lors, il semble pour le moins étrange que les services de renseignements considèrent comme une « attitude de clandestinité » le fait de suivre les recommandations des instances nationales ou européennes visant à protéger la vie privée des Européens contre la surveillance de masse ou l'intelligence économique.

6.3. Une disproportion manifeste dans la conservation des données chiffrées

En l'espèce,

La loi déférée introduit un article L. 822-2 au CSI, ainsi rédigé :

*« **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 ;

7. Audition de M. Bernard Bajolet, directeur général de la sécurité extérieure, sur le projet de loi relatif au renseignement, commission de la défense nationale et des forces armées de l'Assemblée nationale, 24 mars 2015, compte rendu n° 47. Disponible à l'adresse :`http://www.assemblee-nationale.fr/14/cr-cdef/14-15/c1415047.asp`.

« 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. [...] »*

Observons d'emblée que les renseignements chiffrés mentionnés au cinquième alinéa du I de cet article ne peuvent, par définition, pas être des métadonnées. Quand des métadonnées sont chiffrées, elles se présentent alors comme des données, dont on ne peut pas dire ce qu'elles contiennent. Les informations clairement disponibles ne portent que sur le transport (vers où va ce message chiffré, peut-être des informations sur qui pourra le lire). Par définition, les métadonnées sont toujours en clair, puisqu'elles permettent l'acheminement du message chiffré. Les renseignements mentionnés ne peuvent donc, par définition, qu'être des données de contenu, obtenues par des interceptions.

En outre, le fait de porter de trente jours à six ans le délai de conservation pour les renseignements collectés, avec comme seul élément justificatif à ce changement de délai le fait que l'expéditeur du message a suivi les recommandations de l'ANSSI en matière de sécurité est manifestement hors de toute proportion.

Le dernier alinéa de l'article L. 822-2, I, du code de la sécurité intérieure indique par ailleurs que ces données qui, par définition, relèvent du contenu et non de la métadonnée, peuvent être conservées sans aucune limite pour des usages autres que la surveillance des personnes concernées. Si cette conservation peut être envisagée pour les données qui « *contiennent des éléments de cyberattaque* » et donc sont constitutifs des éléments matériels d'une infraction [8], les mots « *ou qui sont chiffrés* » étendent ce dispositif sans justification pour des données qui ne sont pas, *a priori*, en lien avec quelque infraction que ce soit. Cette extension est là encore manifestement disproportionnée.

En conclusion,

En échouant à apporter des garanties nécessaires à la sauvegarde des droits et libertés garantis à l'article 2 et à l'article 11 de la Déclaration de 1789 s'agissant des communications chiffrées, le législateur a méconnu l'obligation qui lui incombe en vertu de l'article 34 de la Constitution.

En conséquence, le cinquième alinéa de l'article L. 822-2, I, du code de la sécurité intérieure ainsi que les mots « *ou qui sont chiffrés* » à l'alinéa suivant doivent être censurés.

8. Et ce bien qu'on puisse s'inquiéter de voir les services de renseignement bénéficier de compétence en matière de cybersécurité alors que la France dispose d'une agence civile dédiée (l'ANSSI).

7. Boîtes noires algorithmiques

À l'article 5 de la loi déférée figurent deux dispositions conçues, selon les dires du directeur général de la DGSE M. Bernard Bajolet, pour « *détecter la préparation d'un attentat terroriste sur notre sol au moyen de l'exploitation de données techniques* » [1].

L'article L. 851-3 concerne ce qui au fil du débat public sur le projet de loi a été qualifié de « boîtes noires algorithmiques », et constitue sans aucun doute la mesure la plus controversée du texte. Il dispose que :

> *« (. . .) Pour les seuls besoins de la prévention du terrorisme, il peut être imposé aux opérateurs et personnes mentionnés à l'article L. 851-1 la mise en œuvre sur leurs réseaux de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste »*

L'article L. 851-2 dispose quant à lui que :

> *« (. . .) Pour les seuls besoins de la prévention du terrorisme, peut être individuellement autorisé le recueil en temps réel, sur les réseaux des opérateurs et personnes mentionnés à l'article L. 851-1, des informations ou documents mentionnés au même article relatifs à une personne préalablement identifiée comme présentant une menace. »*

L'économie générale de ces dispositions a peu évolué au cours de l'examen parlementaire, en dépit des discussions entre le gouvernement et des représentants des plateformes d'hébergement. Outre quelques clarifications sémantiques s'agissant notamment du contrôle de la CNCTR, l'évolution principale tient à la réduction de quatre à deux mois de la durée des autorisations.

Ces deux dispositions semblent destinées à être hautement complémentaires au plan opérationnel :

À travers les boîtes noires algorithmiques installées sur les réseaux des opérateurs de télécommunications (Internet ou téléphone) ou les serveurs des hébergeurs, les services de renseignement pourront scanner l'ensemble des communications transitant par ces infrastructures en vue de déceler certains types de comportements. En séance publique, le ministre de la Défense a indiqué que l'analyse automatique et en temps réel des données de connexion – dont la nature exacte n'est pas précisée dans le texte – devait permettre

1. Audition de M. Bernard Bajolet, directeur général de la sécurité extérieure, sur le projet de loi relatif au renseignement, commission de la défense nationale et des forces armées de l'Assemblée nationale, 24 mars 2015, compte rendu n° 47. Disponible à l'adresse :`http://www.assemblee-nationale.fr/14/cr-cdef/14-15/c1415047.asp`.

de repérer « des connexions à certaines heures, depuis certains lieux, sur certains sites » et « de repérer ainsi un trafic caractéristique » [2].

Quant au directeur de la DGSE, il précise qu'il s'agit de repérer des « attitudes de clandestinité » telles que l'utilisation de protocoles de chiffrement ou d'anonymisation des communications. Lorsque des données de connexion correspondant aux sélecteurs retenus par les services pour configurer leurs algorithmes seront repérées par ces boîtes noires, les sondes prévues par l'article L. 851-2 pourront être activées, ce qui permettra notamment de solliciter directement sur les réseaux des opérateurs téléphoniques et autres fournisseurs d'accès Internet l'identité d'un individu, de connaître en temps réel l'ensemble des données de connexion qui lui sont associées (adresses IP par exemple) mais également de le géolocaliser en temps réel et de tenir une liste complète de ses communications téléphoniques.

Cependant, au plan technique, les explications fournies par le Gouvernement lors des débats parlementaires n'ont pas permis de déterminer exactement quel serait le fonctionnement des boîtes noires algorithmiques. En particulier, les exemples cités ne correspondent pas à ce qu'indiquent les textes. Ainsi, l'exemple de détection de l'usage de méthodes de chiffrement particulières suppose une analyse du contenu, des données, et pas uniquement des métadonnées. En effet, les informations de chiffrement ne sont disponibles qu'en bout de chaîne, chez le destinataire de la communication. Cette information n'est pas visible, ni chez le fournisseur d'accès à Internet, ni chez le fournisseur de service de communication, ni chez l'hébergeur. En pratique, cela induirait nécessairement une analyse en profondeur du contenu (techniques également connues en anglais sous le nom de « *Deep Packet Inspection* »).

De même, l'exemple cité plusieurs fois par le ministre de l'Intérieur, à savoir la détection des individus qui vont consulter des sites sensibles, ne peut être mis en œuvre par analyse des métadonnées que chez les hébergeurs, et non chez les fournisseurs d'accès. La détection porte alors sur un ou plusieurs sites déterminés dont les hébergeurs sont connus de l'administration et soumis au droit français, le but étant d'identifier toutes les personnes qui les consultent. Cette information pourrait au demeurant être obtenue beaucoup plus facilement sans que ne soit portée une atteinte aussi grave aux droits et libertés, en demandant à l'hébergeur du ou des sites en question de fournir toutes les traces de connexion à ce ou ces sites [3].

La mise en œuvre de cette technique revient à collecter la liste des lecteurs, les dates de lecture, et les articles lus sur un site Internet ouvert au public, sans que les lecteurs ne soient *a priori* suspectés de rien. C'est, dans le monde numérique, l'exact équivalent, du recueil de la liste des abonnés d'une publication, et de la surveillance de l'intégralité du lectorat du journal concerné. Cette atteinte ne peut être considérée que comme très sérieuse dans une société démocratique, et doit nécessairement faire l'objet d'un encadrement très strict.

Les explications fournies lors des débats parlementaires n'ont donc pas permis d'éclairer et préciser les principes en vue de l'application concrète du texte, se bornant le plus souvent à décrire les finalités de ces dispositifs sans en préciser les usages, le tout sur

2. Assemblée nationale, deuxième séance du mercredi 15 avril 2015

3. Les traces de connexions permettent de déterminer qui et quand a consulté quelle page d'un site, données que l'hébergeur n'est pas tenu de conserver en vertu de l'article 6 de la LCEN, qui impose la seule conservation des traces de création de contenu, et pas les traces de consultation.

le fondement d'une notion d'||. Ce manque de précision est d'autant plus grave que les dispositions en cause conduisent de fait à une surveillance généralisée, et violent par là même les droits et libertés constitutionnellement garantis.

7.1. Une atteinte généralisée et disproportionnée aux droits et libertés

En obligeant les opérateurs à mettre en œuvre ces dispositifs permettant d'analyser le trafic de manière indiscriminée, le législateur a violé la directive 2000/31/CE relative à certains aspects juridiques des services de la société de l'information. Cette disposition, qui porte une atteinte généralisée dans la vie privée d'une part importante de la population et qui comporte un risque important d'erreurs techniques, renforce le caractère disproportionné de cette technique.

7.1.1. Une obligation générale de surveillance contraire à la directive 2000/31/CE

En droit,

L'article 15, paragraphe 1, de la directive 2000/31/CE sur le commerce électronique dispose que :

> *« Les États membres ne doivent pas imposer aux prestataires, pour la fourniture des services visée aux articles 12, 13 et 14, une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites. »*

Sur ce fondement, dans deux arrêts relatifs à des mesures de filtrage du trafic Internet en vue de détecter et d'empêcher l'échange sans autorisation d'œuvres soumises au droit d'auteur, la CJUE a rejeté des mesures de « surveillance active » de la quasi-totalité des utilisateurs des services concernés (fournisseurs d'accès à Internet dans un cas, réseau social dans l'autre). Selon la Cour de Luxembourg :

> *« (. . .) l'injonction faite au prestataire de services d'hébergement de mettre en place le système de filtrage litigieux l'obligerait à procéder à une surveillance active de la quasi-totalité des données concernant l'ensemble des utilisateurs de ses services. Il s'ensuit que ladite injonction imposerait au prestataire de services d'hébergement une surveillance générale qui est interdite par l'article 15, paragraphe 1, de la directive 2000/31 »*
> (CJUE, 16 février 2012, *SABAM c/ Netlog*, C-360/10, §38. Voir aussi CJUE, 24 novembre 2011, *SABAM c/ Scarlet Extended*, C-70/10, §40.)

Par ailleurs, l'article 88-1 de la Constitution impose au législateur de respecter le droit de l'Union européenne, en disposant que :

> *« La République participe à l'Union européenne constituée d'États qui ont choisi librement d'exercer en commun certaines de leurs compétences en vertu du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne, tels qu'ils résultent du traité signé à Lisbonne le 13 décembre 2007. »*

En l'espèce,

L'article L. 851-3 examiné, paragraphe I, dispose que :

> *« Dans les conditions prévues au chapitre Ier du titre II du présent livre et pour les seuls besoins de la prévention du terrorisme,* ***il peut être imposé aux opérateurs et personnes mentionnés à l'article L. 851-1 la mise en œuvre sur leurs réseaux*** *de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste. »*

Ce faisant, un tel article permet de contraindre les mêmes « prestataires » visés par la directive 2000/31/CE à contribuer à la mise en œuvre de boîtes noires algorithmiques sur leurs réseaux par les services de renseignement.

Or, les éclairages apportés par le Gouvernement aux opérateurs concernés lors de l'examen parlementaire permettent d'établir qu'une telle contribution implique nécessairement de la part de ces prestataires, d'une part, qu'ils installent les dispositifs concernés sur leurs infrastructures et en assurent la maintenance et, d'autre part, qu'ils transmettent les informations retenues par ces algorithmes aux services de renseignement.

Ainsi, en leur imposant de telles démarches, l'article examiné revient précisément à « *imposer aux prestataires [...] une obligation générale de surveiller les informations qu'ils transmettent ou stockent* », en parfaite contradiction des dispositions de l'article 15 de la directive 2000/31/CE et, partant, de l'article 88-1 de la Constitution.

En conclusion,

L'article L. 851-3 du code de la sécurité intérieure doit être censuré, violant l'article 88-1 de la Constitution.

7.1.2. L'analyse automatique des données doit s'interpréter comme une atteinte grave aux libertés

Les défenseurs du projet de loi arguent que l'article L. 851-3 ne saurait aboutir à une surveillance généralisée puisque seule une faible proportion des données de connexion analysées automatiquement par ces dispositifs techniques peuvent faire l'objet d'examens plus approfondis.

En droit,

Pour autant, le Conseil constitutionnel considère 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. Par suite, 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)

Quant à elle, la CEDH considère, de jurisprudence constante, que :

> *« Le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8.* ***Peu importe que les informations mémorisées soient ou non utilisées par la suite****. »*

(CEDH, *S. et Marper c. Royaume-Uni*, 4 décembre 2008, n°30562/04 et 30566/04, §67.)

La Cour de justice de l'Union européenne a elle aussi eu l'occasion de condamner les mesures de surveillance indiscriminées au regard du droit au respect de la vie privée. Dans sa décision du 8 avril 2014 invalidant la directive 2006/24/CE sur la conservation des données de connexion, elle souligne à propos de cette directive que :

> *« Elle s'applique donc* ***même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves****. En outre, elle ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel. »*
>
> (CJUE, 8 avril 2014 *Digital Rights Ireland*, C-293/12, §58.)

En l'espèce,

Les boîtes noires algorithmiques traitent de façon indifférenciée toutes les données traitées par les réseaux ou infrastructures sur lesquels elles sont installées, qui sont nécessairement pour une large part des données à caractère personnel.

Ainsi — même si les moyens techniques modernes permettent de surveiller de manière automatique et en temps réel les comportements des individus sur les réseaux numériques plutôt que de collecter systématiquement et de conserver pour longtemps leurs données — , les outils de « *scanning* » prévus à l'article L. 851-3 aboutissent nécessairement à une ingérence dans la vie privée et dans la liberté de communication, et ce quand bien même l'immense majorité de ces données ne donnerait lieu à aucune utilisation ultérieure.

En conclusion,

Au regard de la jurisprudence des trois juridictions citées, le traitement réalisé par les boîtes noires algorithmiques porte une atteinte indiscriminée au droit au respect de la vie privée de personnes pour lesquelles il n'existe aucun lien direct ou même lointain avec une infraction. Leur mise en œuvre ne peut se faire « de manière adéquate et proportionnée », tel qu'exigé par le Conseil constitutionnel au regard de l'article 34 de la Constitution, ce qui justifie la censure de cette disposition.

7.1.3. Une technique inefficace et dès lors disproportionnée

En droit,

Le Conseil constitutionnel a jugé à propos des mesures d'investigation spéciales en vue de la répression des crimes et délits d'une gravité et d'une complexité particulières que les restrictions qu'elles apportent aux droits et libertés constitutionnellement garantis doivent être non seulement « nécessaires à la manifestation de la vérité » mais surtout, *proportionnées à la gravité et à la complexité des infractions commises et n'introduisent pas de discriminations injustifiées*[4]

De même, la CEDH considère que :

4. 2010-25 QPC, 16 septembre 2010, cons. 11 et 12, Journal officiel du 16 septembre 2010, page 16847, texte n° 64, Rec. p. 220

> *« Une ingérence est considérée comme « nécessaire dans une société démocratique » pour atteindre un but légitime si elle répond à un « besoin social impérieux » et, en particulier, si elle est proportionnée au but légitime poursuivi et si les motifs invoqués par les autorités nationales pour la justifier apparaissent « pertinents et suffisants ». »*
> (CEDH, *S. et Marper c. Royaume-Uni*, 4 décembre 2008, n°30562/04 et 30566/04, §101)

Il en ressort que serait inconstitutionnelle et inconventionnelle une disposition législative permettant une atteinte aux droits et libertés à la fois disproportionnée et non nécessaire à la poursuite des objectifs qu'on lui assigne.

En l'espèce,

Même lorsque les données scannées par les boîtes noires correspondent aux sélecteurs retenus dans la conception des algorithmes, des personnes n'ayant rien à voir avec les finalités de ces dispositions, à savoir la lutte contre le terrorisme, risquent de faire l'objet de mesures de surveillance plus poussées. Ainsi, le simple recours à des protocoles de chiffrement — dont l'utilisation est, comme il a déjà été évoqué, recommandée par les pouvoirs publics, notamment l'Assemblée parlementaire du Conseil de l'Europe (voir section 6.2 page 49) — risque de conduire au traitement, et à la conservation, des données concernées.

Une telle suspicion déclenchera automatiquement la transmission de ces données par les opérateurs ayant installé les boîtes noires aux services de renseignement, lesquels conserveront et analyseront ces données [5]. Sur cette seule base, les services de renseignement pourront ensuite solliciter une autorisation en vue de recueillir en temps réel les informations et documents détenus par les opérateurs (article L. 851-2) ou même réaliser des interceptions de sécurité (article L. 852-1).

Dans le même ordre d'idées, il importe de rappeler que dans les controverses juridiques touchant aux techniques dites de *data-mining* mises en œuvre dans le cadre d'activités de surveillance, de nombreux ingénieurs interviennent pour rappeler le caractère inefficace et contre-productif de ces mesures [6]. Ainsi, au cours du débat parlementaire sur le projet de loi sur le renseignement, une note interne issue d'experts de l'Institut national de recherche en informatique appliquée (Inria) a fuité dans la presse [7]. Dans ce document, les auteurs soulignent que les personnes visées par ces mesures pourront facilement les contourner à travers l'utilisation de techniques de chiffrement ou d'anonymisation des

5. Or, l'article L. 851-3 examiné prévoit, à son II, que la CNCTR « dispose d'un accès direct et permanent à ces traitements ainsi qu'aux informations et données recueillies », impliquant sans ambiguïté que les boîtes noires réalisent « la collecte, l'enregistrement, la conservation, la consultation et la communication » des données qu'elles traitent, même temporaire, sans quoi la CNCTR ne pourrait nullement y accéder. De même, cet article prévoit, à son IV, que « lorsque les traitements [...] détectent des données susceptibles de caractériser l'existence d'une menace à caractère terroriste, le Premier ministre ou l'une des personnes déléguées par lui peut autoriser [...] l'identification de la ou des personnes concernées », impliquant nécessairement que les données permettant cette identification aient été préalablement collectées et conservées.

6. Voir par exemple : Alberson et al., *Amici Curiæ Brief of Experts in Computer and Data Science in Support of Appellants and Reversal*. Cour d'appel du deuxième circuit des États-Unis d'Amérique. Disponible à l'adresse `http://michellawyers.com/wp-content/uploads/2015/01/ACLU-v.-Clapper_Amici-Curiae-Brief-of-Experts-In-Computer-and-Data-Science-In-Support-of-Appellants-and-Reversal.pdf`.

7. Note interne de l'Inria, *Éléments d'analyse technique du projet de loi relatif au renseignement*, 30 avril 2015. Disponible à l'adresse : `http://sciences.blogs.liberation.fr/files/265206918-note-interne-de-l-inria.pdf`.

communications. Ils mettent également en garde contre le risque de « faux-positifs », c'est-à-dire des données détectées à tort par l'algorithme :

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

À ces taux d'erreur s'ajoutent certains éclairages opérationnels comme, par exemple, ceux issus de documents récemment fuités dans la presse par l'intermédiaire d'Edward Snowden. Ces documents internes font état de témoignages d'analystes de la NSA, qui soulignent les difficultés engendrées par la logique des mégadonnées ou « Big Data » dans les activités de l'agence américaine [8]. Cette critique des dispositifs algorithmiques rejoint celles formulées par les ingénieurs et experts en la matière, qui pointent eux aussi le risque de noyer les analystes sous des masses d'informations qui *in fine* les empêchent de mener à bien leurs missions de manière efficace [9].

En conclusion,

Le but même des dispositions en question — qui consistent à surveiller les communications de pans entiers de la population pour détecter des comportements suspects liés à une menace terroriste — n'apparaît évidemment pas légitime, et l'ingérence d'autant moins « nécessaire dans une société démocratique » que le gouvernement n'a pas démontré, contre les arguments avancés par des techniciens, que ces mesures permettaient effectivement d'atteindre l'objectif que le législateur leur assigne. À défaut d'atteindre effectivement l'objectif poursuivi, l'ingérence dans le droit à la vie privée et la liberté de communication de l'ensemble des utilisateurs de ces réseaux est, quant à elle, effective et attestée.

L'article L. 851-3 du code de la sécurité intérieure doit donc être censuré, violant l'article 2 de la Déclaration de 1789 et l'article 34 de la Constitution.

7.2. Un profilage automatisé contraire à la loi informatique et libertés

En droit,

À travers sa jurisprudence, le Conseil constitutionnel a eu l'occasion d'examiner des lois spéciales relatives aux moyens d'enquête et d'investigation au regard de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (dite « loi informatique et libertés ») afin d'en dégager certains principes :

8. Peter Mass, « Inside NSA, Officials Privately Criticize "Collect It All" Surveillance », The Intercept, 28 mai 2015. `https://firstlook.org/theintercept/2015/05/28/nsa-officials-privately-criticize-collect-it-all-surveillance/`.

9. Grégoire Chamayou, « Loi sur le renseignement : les bugs du big data », *Libération*, 14 avril 2015. Disponible à l'adresse : `http://www.liberation.fr/societe/2015/04/14/loi-sur-le-renseignement-les-bugs-du-big-data_1241075`.

> *« Considérant, en outre, qu'en vertu de l'article 2 de la loi du 6 janvier 1978 susvisée, que ne remettent pas en cause les dispositions contestées : « Aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé » ; que les données recueillies dans les fichiers ne constitueront donc, dans chaque cas, qu'un élément de la décision prise, sous le contrôle du juge, par l'autorité administrative ; »*
>
> (Conseil constitutionnel, 2003-467 DC, 13 mars 2003, cons. 34, Journal officiel du 19 mars 2003, page 4789, Rec. p. 211)

Or, la loi du 6 janvier 1978 prévoyait dès sa version initiale, dans son article 2, d'encadrer l'utilisation du profilage informatique. L'article 2 prévoyait ainsi qu'aucune « *décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé* ». Un principe que l'on retrouve aujourd'hui à l'article 10 de la loi, lequel interdit qu'une décision produisant des effets juridiques à l'égard d'une personne soit prise « *sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité* ».

Ce principe est aussi garanti au niveau européen, l'article 15.1 de la directive 95/46/CE [10] disposant que « *les États membres reconnaissent à toute personne le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité* ».

En l'espèce,

La présente loi prévoit que l'article L. 851-3 dispose :

> *« IV. – **Lorsque les traitements mentionnés au I détectent des données susceptibles de caractériser l'existence d'une menace à caractère terroriste, le Premier ministre ou l'une des personnes déléguées par lui peut autoriser**, après avis de la Commission nationale de contrôle des techniques de renseignement donné dans les conditions du chapitre Ier du titre II du présent livre, l'identification de la ou des personnes concernées et le recueil des données y afférentes (...). »*

Dès lors, les traitements automatisés de données ainsi prévus ont pour finalité de permettre à l'administration de prendre une décision — identifier une personne et recueillir les données y afférentes — « sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité » réalisé par les boites noires, contrevenant parfaitement à l'article 10 de la loi informatique et libertés, sans que les dispositions ne garantissent la sauvegarde de l'intérêt légitime des personnes concernées.

En conclusion,

Le IV de l'article L. 851-3 est contraire à l'interdiction de profilage prévue à l'article 10 de la loi informatique et à laquelle le Conseil constitutionnel soumet l'administration, ainsi qu'à l'article 15.1 de la directive 95/46/CE de l'Union européenne que l'article 88-1 de la Constitution imposait au législateur de respecter. **La disposition doit donc pour ce seul motif être censurée.**

10. Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

Subsidiairement,

Toutefois, si le Conseil constitutionnel l'estimait conforme à la loi informatique et libertés et au principe de proportionnalité, il faudrait à tout le moins encadrer cette disposition par une réserve d'interprétation.

Dans son étude annuelle de 2014 sur le numérique et les droits fondamentaux, le Conseil d'État recommandait ainsi l'adoption d'une recommandation de la CNIL ou un avis du G29 pour préciser l'interprétation de l'article 10 de la loi « informatique et liberté », dans le but de s'assurer qu'une intervention humaine dans la prise de décision résultant d'un traitement de données soit présente et ne soit pas que formelle [11].

En l'absence d'une telle décision de la part des autorités administratives en charge de la protection des données personnelles et compte tenu du risque de voir les traitements automatisés prévus par l'article L. 851-3 constituer le seul motif justifiant la mise en œuvre de techniques de recueil de renseignements, le Conseil constitutionnel devrait préciser – par exemple sur le fondement de l'article 7 de la Déclaration de 1789 [12] – permettant de procéder lui-même à cet encadrement du profilage algorithmique.

Cette réserve d'interprétation pourrait notamment préciser que les demandes d'autorisation transmises à la CNCTR doivent obligatoirement faire état d'éléments montrant que la décision d'identification et de recueil de renseignements à l'encontre d'une personne se fonde sur des informations autres que celles fournies par des traitements automatisés de données.

11. Rapport annuel du Conseil d'État, 2014, p. 299.

12. « Nul homme ne peut être accusé, arrêté ni détenu que dans les cas déterminés par la Loi, et selon les formes qu'elle a prescrites. Ceux qui sollicitent, expédient, exécutent ou font exécuter des ordres arbitraires, doivent être punis ; mais tout citoyen appelé ou saisi en vertu de la Loi doit obéir à l'instant : il se rend coupable par la résistance ».

8. Captation de paroles, d'images et de données informatiques

L'article 6 de la loi déférée, insère au chapitre III, un article L. 853-1 au code de la sécurité intérieure, qui dispose que :

> *« I. — Dans les conditions prévues au chapitre Ier du titre II du présent livre, peut être autorisée, lorsque les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé, l'utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel, ou d'images dans un lieu privé. [...] »*

Il est à noter que la définition de cette technique est littéralement identique à celle donnée à l'article 706-96 du code de procédure pénale concernant les mesures d'enquête judiciaire [1].

L'article L. 853-2, I, dispose que :

> *« Dans les conditions prévues au chapitre Ier du titre II du présent livre, peut être autorisée, lorsque les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé, l'utilisation de dispositifs techniques permettant :*
>
> *« 1° D'accéder à des données informatiques stockées dans un système informatique, les enregistrer, les conserver et les transmettre ;*
>
> *« 2° D'accéder à des données informatiques, les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels. »*

Ces deux techniques n'étaient pas autorisées par les dispositions abrogées par la présente loi et qui encadraient jusqu'alors le recours aux techniques de renseignement au titre IV du livre II du CSI. Désormais, les services de renseignement peuvent y recourir pour

1. Art. 706-96 du code de procédure pénale : « Lorsque les nécessités de l'information concernant un crime ou un délit entrant dans le champ d'application de l'article 706-73 l'exigent, le juge d'instruction peut, après avis du procureur de la République, autoriser par ordonnance motivée les officiers et agents de police judiciaire commis sur commission rogatoire à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, la captation, la fixation, la transmission et l'enregistrement de paroles prononcées par une ou plusieurs personnes à titre privé ou confidentiel, dans des lieux ou véhicules privés ou publics, ou de l'image d'une ou plusieurs personnes se trouvant dans un lieu privé. Ces opérations sont effectuées sous l'autorité et le contrôle du juge d'instruction ».

l'ensemble des finalités énoncées à l'article L. 811-3 du CSI tel que créé par la présente loi (voir chapitre 3 page 15). De plus, l'étendue de l'atteinte au droit au respect à la vie privée portée par ces techniques est, elle aussi, particulièrement nouvelle.

En effet, d'une part, il s'agit pour les services de renseignement de poser des dispositifs d'enregistrement de paroles et d'images dans des lieux privés, voire directement dans des lieux d'habitation, ce qui n'était jusqu'à présent autorisé que dans le cadre et sous les garanties de la procédure pénale pour constater des infractions précisément définies.

D'autre part, les nouveaux dispositifs techniques de captation de données informatiques s'apparentent directement à l'exploitation de logiciels malveillants à l'insu des utilisateurs, étant destinés à prendre la maîtrise des machines qu'ils infectent contre la volonté de leurs utilisateurs. Notamment, est ainsi directement fait référence au logiciel espion notoire désigné de *keylogger*, ou d'enregistreur de frappe, enregistrant chronologiquement l'ensemble des frappes réalisées sur le clavier d'une machine afin de collecter à la source toute information y étant entrée, en ligne comme en local, avant que l'utilisateur ne puisse recourir à la moindre technique informatique de protection.

Enfin, la gravité particulière des atteintes portées par ces techniques ressort nettement de ce que le législateur a entendu ne les autoriser seulement « lorsque les renseignements ne peuvent être recueillis par un autre moyen ».

Or, ni le champ matériel de ces dispositions ni les conditions de mises en œuvre ne sont clairement définis, ce qui les entache d'**incompétence négative**, tandis que le législateur a échoué à apporter à ces techniques de renseignement des garanties suffisantes pour les droits et libertés constitutionnellement garantis.

8.1. Le champ matériel de ces techniques n'est pas défini

La notion de « système informatique » employée par le législateur au 1° de l'article L. 853-2, I, n'est définie ni par la présente loi ni par aucune autre disposition légale. Toutefois, il semble qu'il faille la distinguer de celle de « système de traitement automatisé de données », employée par le législateur à l'alinéa suivant, une telle distinction ne pouvant être de nul effet.

Or, cette seconde notion est déjà mobilisée par la loi, au chapitre III, intitulé « des atteintes aux systèmes de traitement automatisé de données », titre II, livre III du code pénal, qui n'en donne certes pas de définition mais a permis aux juges d'en décrire progressivement les contours. C'est ainsi qu'un radiotéléphone [2], un disque dur [3], le réseau France Télécom et le réseau de Carte bancaire [4] constituent des « systèmes de traitement automatisé de données ».

De ces différentes interprétations, on peut déduire que la notion « systèmes de traitement automatisé de données » recouvre tout équipement permettant l'acquisition automatique, le stockage, la manipulation, le contrôle, l'affichage, la transmission, ou la

2. Cour d'appel de Toulouse, 17 décembre 2008, n° 07/01177.

3. Cour d'appel de Douai, 28 mai 2010 n° 09/02731.

4. Tribunal correctionnel Paris, 25 février 2000. Disponible à cette adresse : `http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=1200`.

réception de données informatiques.

Dès lors, le sens de la notion de « système informatique », nécessairement distincte de cette définition-ci, en devient particulièrement incertain : recouvre-t-il une variété d'équipements plus réduite, plus large ou entièrement différente que ceux couverts par la notion de « systèmes de traitement automatisé de données » tels que définis par la jurisprudence judiciaire, et selon quels critères ?

En conclusion,

En choisissant la notion de « système informatique » sans fournir aucun élément pour en préciser le sens, le législateur a privé les citoyens de pouvoir connaître, même approximativement, la portée du 1° de l'article L. 853-2, I, et a ainsi permis aux services de renseignement de fixer seuls l'étendue des atteintes au droit à la vie privée et à la liberté de communication en résultant.

Le 1° de l'article L. 853-2, I, inséré au code de la sécurité intérieure par la loi déférée est entaché d'incompétence négative, le législateur ayant manqué à l'obligation que lui incombe l'article 34 de la Constitution de produire, en vue des articles 4, 5, 6 et 16 de la Déclaration de 1789, d'établir des normes intelligibles et accessibles, et doit ainsi être censuré.

8.2. L'imprécision des conditions de mise en œuvre

En droit,

L'article L. 706-73 du code de procédure pénale, tel que modifié par l'article 13 de la loi n° 2014-790 du 10 juillet 2014, édicte une liste exhaustive des infractions justifiant la mise en place d'un dispositif aussi attentatoire au droit au respect de la vie privée.

La Cour de cassation avait déjà confirmé à cet égard, dans un arrêt du 23 novembre 1999 (n° 99-82.658), que le juge d'instruction ne pouvait autoriser un tel dispositif que dans la mesure où il ne portait pas atteinte aux droits de la défense, le respect strict de la liste exhaustive des infractions de l'article 706-73 constituant à cet égard une garantie.

Le Conseil constitutionnel a émis une réserve d'interprétation de portée générale pour l'article 1er de la loi portant adaptation de la justice aux évolutions de la criminalité. Cette réserve précise qu'il appartient à l'autorité judiciaire de mettre en œuvre les procédures prévues à cet article, en veillant, au cas par cas, à ce que les mesures soient nécessaires et proportionnées aux besoins de l'enquête.

> *« Considérant que les procédures spéciales définies par l'article 1er de la loi déférée sont de nature à affecter gravement l'exercice de droits et libertés constitutionnellement protégés, tels que la liberté individuelle, l'inviolabilité du domicile et le secret de la vie privée ; que l'autorité judiciaire, gardienne de la liberté individuelle, ne saurait dès lors autoriser leur utilisation que dans la mesure nécessaire à la recherche des auteurs d'infractions particulièrement graves et complexes, elle-même indispensable à la sauvegarde de principes et droits de valeur constitutionnelle.*
>
> *« Considérant que, pour décider de mettre en œuvre l'une de ces procédures, l'autorité judiciaire doit disposer d'une ou plusieurs raisons plausibles de soupçonner que les faits constituent l'une des infractions énumérées par l'article 706-73 nouveau du code de*

procédure pénale [...]. »
(Cons. const., DC n° 2004-492 DC du 2 mars 2004, §69 et §70)

La mise en œuvre de ces procédures spéciales doit ainsi reposer sur un motif suffisant et respecter strictement la liste des infractions énumérées par l'article 706-73 du code de procédure pénale, afin de garantir les droits de la défense et les libertés individuelles.

À travers sa jurisprudence sur les interceptions de communications, la CEDH impose également une forte exigence de « qualité de la loi » pour prévenir les atteintes au droit au respect de la vie privée protégé par l'article 8 de la Convention. La CEDH rappelle ainsi dans l'arrêt *Bykov c/ Russie* du 10 mars 2009 :

« La loi doit user de termes assez clairs pour indiquer aux individus de manière suffisante en quelles circonstances et sous quelles conditions elle habilite les autorités publiques à prendre pareilles mesures secrètes »
(CEDH, *Bykov c. Russie*, 10 mars 2009, n° 378/02, §76)

Dans l'affaire *Malone c. Royaume-Uni*, elle estime également que :

« Puisque l'application des mesures de surveillance secrète des communications échappe au contrôle des intéressés comme du public, la « loi » irait à l'encontre de la prééminence du droit si le pouvoir d'appréciation accordé à l'exécutif – ou au juge – ne connaissait pas de limites. En conséquence, elle doit définir l'étendue et les modalités d'exercice d'un tel pouvoir avec une netteté suffisante pour fournir à l'individu une protection adéquate contre l'arbitraire »
(CEDH, *Malone c. Royaume-Uni*, 2 août 1984, n°8691/79, §67)

Ainsi, l'utilisation d'un enregistrement dissimulé comme preuve à charge dans le cadre d'une procédure pénale constitue une violation de ces articles lorsque le système d'écoute n'a pas été prévu par la loi [5].

La CEDH avait déjà précisé que les écoutes téléphoniques devaient être analysées en une *ingérence de l'autorité publique* dans l'exercice d'un droit. Cette ingérence pouvant néanmoins se justifier, au regard de l'article 8 de la CESDH si elle est prévue par la loi.

« Il reste à examiner si l'ingérence était « nécessaire dans une société démocratique » pour atteindre ces objectifs. Selon la jurisprudence constante de la Cour, les États contractants jouissent d'une certaine marge d'appréciation pour juger de l'existence et de l'étendue de pareille nécessité, mais elle va de pair avec un contrôle européen portant à la fois sur la loi et sur les décisions qui l'appliquent, même quand elles émanent d'une juridiction indépendante »
(CEDH, *Lambert c/ France*, 24 août 1998, §30).

Ces procédés très intrusifs ne sont légitimes que s'ils sont autorisés par une loi qui détermine elle-même précisément les cas et les procédures selon lesquelles le pouvoir exécutif peut y recourir. Une loi de qualité au sens de la CEDH impliquerait de limiter les procédés des articles 853-1 et 853-2 du CSI à certaines des finalités de 811-3, et de prévoir une procédure d'autorisation ou de contrôle qui permet de s'assurer au cas par cas de la proportionnalité de l'intrusion. Ainsi, un contrôle de proportionnalité opéré par la CEDH est nécessaire, et ce, même si une telle décision émane d'une autorité judiciaire indépendante. Ces exigences devraient donc être les mêmes dans le cas où une telle ingérence est décidée par une autorité administrative.

5. Voir CEDH, *Bykov c/ Russie*, 10 mars 2009.

La CEDH a par ailleurs eu l'occasion de condamner la France à deux reprises pour des sonorisations antérieures à l'entrée en vigueur de la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité. La France a par exemple été sanctionnée pour la violation de l'article 8 de la CESDH concernant la sonorisation de l'appartement d'un tiers, dans lequel le requérant s'était rendu. La CEDH estime dans cet arrêt que :

> *« (...) comme les interceptions d'entretiens téléphoniques, les écoutes de conversations par le biais de la pose de micros représentent une atteinte grave au respect de la vie privée. Elles doivent donc se fonder sur une « loi » d'une précision particulière : dans ce domaine aussi, l'existence de règles claires et détaillées apparaît indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner (...). Selon la Cour, la « loi » doit offrir aux justiciables « des sauvegardes adéquates » contre les abus à redouter (...), de même nature qu'en matière d'écoutes téléphoniques »*
> (CEDH, *Vetter c/ France*, 31 mai 2005, n° 59842/00, §26)

La Cour souligne en outre que « *les catégories de personnes susceptibles de faire l'objet d'une telle mesure et* ***la nature des infractions*** *pouvant y donner lieu doivent être définies* » (§27).

La CEDH a également jugé illégal un dispositif de sonorisation au regard de l'article 8 de la convention, dans un parloir d'une maison d'arrêt. L'enregistrement est considéré dans ce cas comme une ingérence dans la vie privée du détenu et de ses proches car il n'est pas prévu par la loi, au sens de l'article 8 §2 de la convention (CEDH, *Wisse c/ France*, 20 décembre 2005). La Cour rappelle dans cet arrêt que :

> *« (...) Les mots « prévue par la loi », au sens de l'article 8 §2, veulent d'abord que la mesure incriminée ait une base en droit interne (...). À l'instar des interceptions d'entretiens téléphoniques ou des écoutes de conversations par le biais de la pose de micros, la loi sur laquelle il se fonde doit être prévisible quant au sens et à la nature des mesures applicables (...). Parmi les « sauvegardes adéquates » contre les abus à redouter figurent les catégories de personnes susceptibles de faire l'objet d'une telle mesure et la nature des infractions pouvant y donner lieu doivent être définies »*
> (CEDH, *Wisse c/ France*, 20 décembre 2005, n° 71611/01, §33)

La CEDH exige dans ces deux arrêts que le droit français indique de manière suffisamment claire les possibilités d'ingérence des autorités dans la vie privée des personnes poursuivies, ainsi que l'étendue et les modalités d'exercice de leur pouvoir d'appréciation dans ce domaine. **La loi doit donc définir avec précision la nature des infractions pouvant donner lieu à l'utilisation de ces dispositifs**.

En l'espèce,

Or, si une liste précise d'infractions est bien établie dans le code de procédure pénale afin de justifier l'utilisation de ces techniques, tel n'est pas le cas dans le code de sécurité intérieure.

En effet, les nouvelles dispositions du code de la sécurité intérieure ne prévoient pas de liste d'infractions justifiant le recours par les services spécialisés de renseignement aux techniques mentionnées dans le titre V, du livre VIII, notamment la sonorisation et captation (voir chapitre 3 page 15).

Les systèmes de sonorisation et de captation peuvent ainsi être utilisés très largement, en fonction des intérêts mentionnés à l'article L. 811-3, alors même que ces différentes finalités recouvrent des missions générales qui ne sauraient constituer des infractions telles

qu'exigées par les juges du Conseil constitutionnel et de la CEDH. Une infraction doit réunir trois éléments, soit un élément légal, un élement matériel et un élément moral. Or, pour rappel, parmi les finalités pour lesquelles ce dispositif peut être utilisé, on trouve notamment :

1. *Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère*
2. *Les intérêts économiques, industriels et scientifiques majeurs de la France*

Clairement, ces « finalités » ne comportent ni élément matériel, ni élément moral clairement définis par la loi. Ces intérêts ne peuvent donc pas être qualifiés d'infractions. En droit, ces finalités ne suffisent pas à justifier le recours à de telles techniques sans constituer une atteinte à l'inviolabilité du domicile et au droit de la défense, puisqu'une marge de manœuvre trop importante est ainsi laissée au pouvoir exécutif et à la CNCTR.

Il faut observer que le seul fait de limiter le recours à ces procédés aux cas dans lesquels ils apparaîtraient comme le seul moyen d'obtenir les renseignements est une limitation insuffisante, dès lors que c'est le Premier ministre qui détermine seul si une telle condition est remplie. La limitation temporelle est également inopérante dès lors que leur renouvellement consécutif n'est nullement limité. Enfin, la loi conduit à une disproportion manifeste en permettant le recours aux techniques de sonorisation pour la sauvegarde *et la « **promotion** »* des intérêts fondamentaux de la Nation plutôt que pour leur seule sauvegarde (article L. 811-3).

En conclusion,

En l'absence d'indications sur la nature exacte des infractions pouvant conduire à l'autorisation de mettre en œuvre les techniques particulièrement intrusives de captation de paroles, d'images et de données informatiques, le fait que la loi permette de recourir à ces procédés pour l'ensemble des finalités de l'article L. 811-3 porte une atteinte particulièrement grave aux droits et libertés constitutionnellement garantis.

Les articles L. 853-1 et L. 853-2 créés par la loi déférée sont dès lors entachés d'incompétence négative, le législateur ayant manqué à l'obligation d'assurer une juste conciliation entre les intérêts poursuivis par la présente loi et le respect des droits et libertés fondamentaux des citoyens. Ils doivent être censurés.

9. Mesures de surveillance des communications internationales

Ce chapitre examine les régimes spéciaux résultant de l'article L. 854-1 relatif aux mesures de « surveillance internationale ». Ces dispositions posent plusieurs problèmes liés à l'inintelligibilité de la loi, aux graves insuffisances du contrôle exercé sur ces mesures, ainsi qu'à la remise en cause de l'universalité des droits affirmée à la fois à l'article premier de la Déclaration de 1789 et dans le bloc de conventionnalité.

À titre préliminaire, il convient de rappeler qu'en dépit de l'appellation du chapitre IV dans lequel est inclus l'article L. 854-1, son champ d'application est réduit à la surveillance des communications « émises ou reçues » hors du territoire national uniquement lorsque les opérations de recueil, de traitement, de conservation, d'exploitation ou de destruction sont conduites sur le territoire national [1]. En est donc exclue toute surveillance (collecte, enregistrement ou exploitation de renseignements) réalisée par les services français à l'extérieur du territoire, même concernant des Français.

Ensuite, pour les communications internationales soumises à des mesures de surveillance, l'article L. 854-1 instaure un double régime. Le premier régime apporte certaines garanties aux « *correspondances interceptées [qui] renvoient à des numéros d'abonnement ou à des identifiants techniques* ***rattachables au territoire national*** *ou à des personnes qui faisaient l'objet d'une autorisation d'interception de sécurité en application de l'article L. 852-1 à la date à laquelle elles ont quitté le territoire national* ». Le second régime concerne les communications internationales qui ne sont pas rattachables au territoire national, pour lesquelles les garanties sont largement amoindries.

En résumé, il ressort que la loi aboutit au total à pas moins de quatre régimes distincts pour l'interception des communications et autres correspondances :

- la surveillance des communications émises et reçues sur le territoire national lorsqu'elle est conduite sur le territoire national (régime de « droit commun » régi par le titre II créé par la loi) ;
- la surveillance des communications rattachables au territoire national mais émises *ou* reçues à l'étranger lorsqu'elle est conduite en tout ou en partie *sur* le territoire national (régi par l'article L. 854-1-II) ;
- la surveillance des communications émises ou reçues à l'étranger qui ne sont pas

1. Voir : Zone d'Intérêt, « Un projet de loi qui n'inquiète pas le renseignement extérieur », 17 avril 2015. Disponible à l'adresse : `http://zonedinteret.blogspot.fr/2015/04/un-projet-de-loi-qui-ninquiete-pas-le.html`.

rattachables au territoire national, lorsqu'elle est conduite sur le territoire national (régie par l'article L. 854-1) ;
– la surveillance de toute communication émise *et* reçue à l'étranger ainsi que la surveillance de toute communication (qu'elle soit émise ou reçue en France, même si elle est rattachable au territoire national, voire émise *et* reçue en France mais transitant hors des frontières nationales dès lors que ces opérations de surveillance ont lieu hors des frontières nationales, lesquelles ne font l'objet d'aucun encadrement législatif, **y compris lorsqu'elles concernent des citoyens français** (les expatriés n'étant nullement protégés).

En vertu de l'article L. 854-1 sur la surveillance internationale, les agences de renseignement françaises pourront légalement, à l'instar de leurs homologues anglo-saxonnes, intercepter massivement les flux internationaux partout dans le monde (c'est-à-dire correspondant aux trois derniers cas mentionnés ci-dessus), France comprise, pour ensuite stocker, traiter et analyser ces données sur le territoire national, notamment dans les locaux franciliens de la DGSE. Des garanties *a minima*, dérogatoires au droit commun, seront applicables aux communications internationales rattachables au territoire national (troisième cas mentionné ci-dessus) lorsque les opérations de surveillance ont lieu depuis la France (voir *infra*).

Le dispositif ainsi créé permettra l'aspiration massive de communications en provenance ou à destination de l'étranger qui pourront pour nombre d'entre elles être conservées indéfiniment. De fait, la disposition semble calquée sur la section 702 de la loi américaine FISA, qui est au cœur des controverses autour des révélations d'Edward Snowden. Elle rappelle également le droit applicable au Royaume-Uni ou en Allemagne.

Au final, ces dispositions sur la surveillance des communications internationales pêchent sur plusieurs points qui justifient leur censure. Sont particulièrement en cause l'inintelligibilité de la loi, l'absence de contrôle préalable des communications « émises ou reçues à l'étranger » même lorsqu'elles sont rattachables au territoire national, et la violation de l'universalité des droits affirmée notamment à l'article premier de la Déclaration de 1789.

9.1. Notions de communication internationale, et de lieu d'émission ou de réception

La loi déférée mobilise à de nombreux endroits des notions qui ne sont pas toujours claires sur l'origine ou la destination des communications. Même la réalité technique, indépendamment du contexte juridique, ne fournit pas toujours un éclairage univoque sur ces notions. Un exposé succinct sur le sujet semble nécessaire pour essayer de comprendre, à la lumière des techniques de communication du 21^{e} siècle, la portée des différentes notions utilisées dans le texte.

Pour la clarté de l'exposé on s'en tiendra au seul exemple du courrier électronique. Mais l'ensemble des principes exposés ici s'applique de manière similaire à tous les systèmes permettant l'échange d'un message, ou d'une communication directe (voix, vidéo), entre des utilisateurs.

9.1.0.0.1 Source et destination réelle de la communication La première difficulté est de comprendre la notion de communication. Au niveau le plus haut, on doit forcément considérer que le courrier a pour origine l'utilisateur qui l'écrit, et pour destination l'utilisateur à qui le courrier est adressé. Si l'on cherche alors à définir la notion de communication *émise ou reçue* de l'étranger, on s'intéresse au lieu où se trouve l'auteur du message quand il l'envoie, et au lieu où se trouve le destinataire quand il le lit. Un courrier électronique échangé entre deux personnes qui sont en France est alors considéré comme émis *et* reçu en France.

9.1.0.0.2 Stockage du message Techniquement, ce message est en réalité transmis au serveur qui stocke la boîte aux lettres du destinataire. Ainsi, si ce serveur est à l'étranger, bien que le destinataire soit en France, le courrier électronique est sorti de France, pour aller être rangé dans la boîte du destinataire, où il sera lu. On a alors deux *demi-communications*, si l'on peut dire, l'une sortant de France, pour expédier le message, l'autre entrant en France pour consulter le message. Du point de vue de l'utilisateur, le message est bien émis *et* reçu en France, mais il est simplement *stocké hors du territoire national*, et pour ce faire le message a été transmis hors de France. Il devient délicat de savoir sous lequel des quatre régimes exposés précédemment il doit être considéré.

9.1.0.0.3 Transport du message Si l'on descend un peu plus bas dans la méthode d'acheminement du message, il est en réalité envoyé par l'outil de messagerie de l'expéditeur au serveur qui achemine son courrier sortant [2]. Ce serveur d'acheminement transmettra le message au serveur de réception de la plateforme de messagerie du destinataire, qui lui-même fera en sorte que le message soit stocké dans la bonne boîte aux lettres.

Sur Internet, l'acheminement des communications suit un parcours qui n'est pas toujours aussi simple qu'il n'y paraît. Ainsi, le chemin le plus court de Strasbourg à Paris peut tout à fait passer par les très gros nœuds d'interconnexion d'Amsterdam ou de Francfort. Ainsi, si on suppose que le serveur d'acheminement de l'expéditeur est à Strasbourg, et que le serveur de réception du destinataire est à Paris, la communication entre les deux serveurs pour acheminer le message peut tout à fait *transiter à l'étranger*. Dans ce cas de figure, alors que l'ensemble des acteurs sont en France (expéditeur, destinataire, plateforme de messagerie de l'expéditeur, plateforme de messagerie du destinataire), la communication transite à l'étranger, et il est délicat de dire sous lequel des quatre régimes se trouve le message lors de son acheminement.

Par la suite, la connexion entre l'ordinateur du destinataire et le serveur qui stocke sa boîte aux lettres pose la même difficulté : une connexion de Grenoble à Paris peut très raisonnablement transiter par le nœud d'interconnexion du CERN, à Genève [3]. La communication devient alors « internationale » lors de la lecture du courrier, plutôt que lors de son acheminement : il y a bien une communication entre l'outil de lecture et le serveur de stockage qui *transite par l'étranger*.

2. Le serveur dit SMTP dans la configuration du logiciel. En général celui de son fournisseur de messagerie, que ce soit le serveur de l'entreprise, ou celui de son fournisseur d'accès, ou celui d'une plateforme de messagerie comme Facebook, Hotmail ou Gmail.

3. Les nœuds d'interconnexion cités, Amsterdam, Francfort, Genève, sont en effet parmi les plus importants d'Europe, avec ceux de Londres et de Paris.

9.1.0.0.4 Complexité des grandes plateformes Enfin, la réalité technique est parfois plus complexe. Ainsi, pour les grandes plateformes internationales, il est fréquent que des serveurs intermédiaires stockent des copies. Par exemple que le stockage de la boîte aux lettres soit fait sur le serveur qui semble le plus proche du destinataire, alors qu'une archive complète sera conservée sur les serveurs de référence, aux États-Unis, ou simplement ailleurs en Europe. Ainsi, le message, après avoir été stocké au plus près du destinataire, sera copié sur les serveurs principaux, pour être accessible même si le destinataire souhaite le consulter ailleurs que depuis son lieu de consultation habituel. Le même message se retrouve alors stocké dans plusieurs pays, et acheminé par un nombre d'autant plus grand de points d'interconnexion.

Les systèmes de messagerie instantanée posent exactement le même problème. Ainsi un message direct envoyé *via* Twitter à quelqu'un qui se trouve dans la même ville sera très probablement archivé sur un des serveurs centraux de Twitter, aux États-Unis ou ailleurs en Europe, en transitant potentiellement par plusieurs pays, alors que la communication réelle se fait entre deux personnes qui sont sur le territoire national, si ce n'est carrément dans la même pièce.

Au final, il est ainsi probable que la très grande majorité des communications passant par Internet entre deux personnes qui sont en France soit, à un moment ou à un autre, à un titre ou à un autre, considérée comme des communications *émises ou reçues* de l'étranger.

9.2. Le silence et l'imprécision de la loi nuisent à son intelligibilité

Deux aspects au moins de l'article 854-1 contreviennent à l'objectif constitutionnel d'intelligibilité de la loi en ce qu'ils interdisent aux citoyens d'avoir une « connaissance suffisante » des dispositions dont ils peuvent faire l'objet.

9.2.1. Les modalités de mise en œuvre de la surveillance nationale ne feront l'objet d'aucune publicité

Le premier tient au caractère secret des modalités de surveillance des communications internationales. L'article 854-1-I dispose en effet que :

> *« Un décret en Conseil d'État* ***non publié****, pris après avis de la Commission nationale de contrôle des techniques de renseignement et porté à la connaissance de la délégation parlementaire au renseignement, précise, en tant que de besoin,* ***les modalités de mise en œuvre de la surveillance des communications*** *prévue au présent I ».*

Dans sa jurisprudence relative aux pratiques de surveillance des communications internationales, la CEDH a déjà souligné que :

> *« (...) les États peuvent divulguer certains aspects du fonctionnement d'un dispositif de surveillance extérieure sans compromettre la sécurité nationale [...]. (...) Faute d'avoir défini avec la* ***clarté requise*** *l'étendue et les modalités d'exercice du pouvoir d'appréciation considérable conféré à l'État en matière d'interception et d'analyse des com-*

munications à destination ou en provenance de l'étranger, la loi en vigueur à l'époque pertinente n'offrait pas une protection suffisante contre les abus de pouvoir ».
(CEDH, *Liberty c. Royaume-Uni*, n° 58243/00, 1er octobre 2008, §§68 et 69.)

La Cour sanctionnait alors le Royaume-Uni pour ne pas avoir assuré la prévisibilité de la loi sur laquelle se fondaient ces opérations de surveillance internationale.

Si la loi déférée prétend répondre à cet impératif d'intelligibilité et de prévisibilité de la loi en prévoyant un décret public pour définir notamment « *les conditions d'exploitation, de conservation et de destruction des renseignements collectés, ainsi que les conditions de traçabilité et de contrôle par la Commission nationale de contrôle des techniques de renseignement de la mise en œuvre des mesures de surveillance* », seul un décret non publié est prévu pour préciser les modalités concrètes de ces opérations de surveillance, dont la publicité est pourtant essentielle pour apporter une connaissance suffisante quant à la portée des dispositions législatives en question.

Le choix de la voie réglementaire pour préciser ces différents aspects touchant directement aux droits et libertés constitutionnellement garantis pose d'emblée la question de l'incompétence négative du législateur. Mais s'agissant de l'intelligibilité et de la prévisibilité de la loi, c'est surtout le choix d'un décret secret pour préciser les modalités de la surveillance internationale, et notamment les règles en matière de recueil des renseignements, qui pose problème.

Pour illustrer l'exigence de transparence qu'implique la notion de prévisibilité de la loi, il est utile de se référer à la décision du 6 février 2015 par laquelle le tribunal chargé du contrôle des interceptions de sécurité au Royaume-Uni — le *Investigatory Powers Tribunal* —, a jugé qu'en échouant à assurer la publicité des règles permettant au GCHQ d'accéder aux données collectées par la NSA sur les citoyens britanniques, les pouvoirs publics avaient contrevenu à cette exigence conventionnelle [4].

9.2.2. Les notions clés de « réception » et d'« émission » ne sont pas clairement définies

Outre cette absence de transparence qui nuit à l'intelligibilité du texte, la loi déférée échoue à préciser la nature exacte des communications internationales concernées en ne définissant pas la portée des *notions d'émission ou de réception à l'étranger*. Comme il a été vu au point 9.1 page 70, il y a de nombreuses interprétations possibles de cette notion, sans que la loi vienne expliciter laquelle doit être prise en compte.

De toute évidence, la notion de « communication *émise ou reçue* à l'étranger » est « *susceptible d'au moins deux interprétations* » et contrevient dès lors à la jurisprudence constitutionnelle [5].

En conclusion,

4. "(...) the regime governing the soliciting, receiving, storing and transmitting by UK authorities of private communications of individuals located in the UK, which have been obtained by US authorities pursuant to Prism and/or (on the Claimants' case) Upstream, contravened Articles 8 or 10 ECHR". Investigatory Powers Tribunal, *Liberty and others c. Secretary of State for Foreign and Commonwealth Affairs & Other*, 6 février 2015. Disponible à l'adresse : `http://www.ipt-uk.com/docs/Liberty_Ors_Judgment_6Feb15.pdf`.

5. Conseil constitutionnel, Décision n° 85-191 DC, 10 juillet 1985, cons. 5.

Pour sanctionner ces silences et imprécisions du texte de loi qui mettent en cause son intelligibilité, le Conseil constitutionnel est fondé à censurer l'ensemble des dispositions ayant recours à la notion de « communications qui sont émises ou reçues à l'étranger ».

9.3. L'absence de contrôle des mesures de surveillance des communications « internationales » rattachables au territoire national et des accords d'échanges de données

Outre ces lacunes, l'article L. 854-1 instauré par la loi déférée contrevient également aux règles constitutionnelles et conventionnelles relatives au contrôle des opérations de surveillance secrète (jurisprudence citée dans le chapitre 10 page 85).

9.3.1. Un régime dérogatoire s'agissant des délais de conservation

Certes, notamment grâce à certains amendements parlementaires, les communications internationales rattachables au territoire français (correspondances et données de connexion) sont soumises aux conditions de droit commun prévues pour les mesures de surveillance nationale s'agissant de leur conservation, de leur exploitation et de leur destruction (articles L. 822-2 à L. 822-4), qui s'exercent normalement sous le contrôle de la CNCTR.

En revanche, le délai de conservation des correspondances court à compter de leur première exploitation et non de leur recueil, sans qu'aucun élément ne vienne justifier un tel régime dérogatoire et au mépris de l'universalité des droits (voir les développements *infra*, section 9.4 page 76).

Surtout, **le recueil des communications internationales, même lorsqu'elles sont rattachables au territoire national, peut, en premier lieu, intervenir sans aucun contrôle préalable**.

9.3.2. L'absence de contrôle préalable

En effet, bien que législateur ait tenu à amender le texte de loi pour expliciter la nature des autorisations des opérations de surveillance internationale [6], il n'a pas prévu de soumettre ces dernières à un avis préalable de la CNCTR.

6. L'article L. 851-4 tel qu'amendé par le Parlement précise notamment : « Les autorisations de surveillance des communications concernées et les autorisations d'exploitation ultérieure des correspondances désignent les systèmes de communication, les zones géographiques, les organisations ou les personnes ou groupes de personnes objets de la surveillance, la ou les finalités justifiant cette surveillance ainsi que le ou les services spécialisés de renseignement qui en sont chargés ».

9.3.3. Le manque d'effectivité du contrôle a posteriori

Outre l'absence d'avis préalable de la CNCTR, son contrôle *a posteriori* est, en second lieu, privé d'effectivité.

Certes, suite à un amendement sénatorial, l'article L. 854-1-I dispose que :

> *« Un décret en Conseil d'État, pris après avis de la Commission nationale de contrôle des techniques de renseignement, définit les* ***conditions d'exploitation, de conservation et de destruction des renseignements collectés, ainsi que les conditions de traçabilité et de contrôle par la Commission nationale de contrôle des techniques de renseignement*** *de la mise en œuvre des mesures de surveillance ».*

Pour autant, non content d'entacher cette disposition d'incompétence négative en renvoyant à un acte réglementaire la définition des garanties qu'il lui revenait d'édicter, le législateur prive un tel futur décret de toute effectivité en adoptant l'article L. 833-2-1-5° qui exclut que la CNCTR puisse opérer un contrôle *a posteriori* efficace. Ce dernier prévoit en effet que :

> *« [La CNCTR] 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*** *».*

L'absence d'encadrement du recueil de données de connexion dès lors qu'elles ne sont pas associées à des correspondances

Enfin, la différence instituée par l'article L. 854-1, I, alinéa 2 entre les notions de correspondances et de communications (qui inclut non seulement les correspondances mais également les données de connexion) laisse place à une absence d'encadrement du recueil, de la conservation et de l'exploitation de certaines données de connexion. En effet, seules les correspondances interceptées renvoyant « *à des numéros d'abonnement ou à des identifiants techniques rattachables au territoire national* » ainsi que les données de connexion qui y sont associées bénéficient des garanties prévues aux articles L. 852-1 et L. 822-2 à L. 822-4 (exploitation, conservation, destruction) sous le contrôle de la CNCTR. *Les données de connexion, même lorsqu'elles sont rattachables au territoire national, pourront donc être massivement recueillies dès lors qu'elles ne sont associées à aucune correspondance, et ce sans aucune des modalités de contrôle* a minima *prévues par le II du présent article.*

Ainsi, *via* cette disposition L. 854-1 et dans la mesure où la notion d'émission et de réception des communications s'entend au plan strictement technique (cf. *supra* 9.1 page 70), les services de renseignement pourront contourner l'essentiel des garanties apportées par la loi aux citoyens et résidents français pour leurs communications nationales, et ce alors même que l'émetteur et le destinataire des communications échangées sont situés physiquement sur le territoire français. S'agissant d'Internet, la majorité des communications nationales sont ainsi susceptibles d'échapper au régime de droit commun. Le régime d'exception prévu à l'article L. 854-1 risque ainsi de devenir la règle.

L'absence de contrôle sur les données échangées avec des services étrangers

Notons pour finir que le législateur a fait le choix de soustraire à toute forme de contrôle les données et autres renseignements auxquels les services français auraient eu accès au travers des accords de coopération avec d'autres agences de renseignement.

Ainsi, alors que les révélations du lanceur d'alerte Edward Snowden ont montré que les agences anglo-saxonnes utilisaient les systèmes techniques des agences partenaires pour contourner le droit national et que la DGSE française est engagée dans ces processus de coopération [7], le 4° de l'article L. 833-2 de la loi dispose que :

> *« [La CNCTR] peut solliciter du Premier ministre tous les éléments nécessaires à l'accomplissement de ses missions,* ***à l'exclusion des éléments communiqués par des services étrangers ou par des organismes internationaux*** *ou qui pourraient donner connaissance à la commission, directement ou indirectement, de l'identité des sources des services spécialisés de renseignement (...). »*

En conclusion,

En se refusant à prévoir dans la loi un contrôle préalable et effectif des communications émises ou reçues à l'étranger quand bien même celles-ci concerneraient directement des résidents et des citoyens français, le législateur a violé la Constitution.

9.4. La loi viole l'universalité des droits

9.4.1. Rappels sur la remise en cause de la distinction national/international dans le droit des activités de surveillance et de renseignement

La moindre protection des communications émises ou reçues à l'étranger et l'absence de protection pour les communications interceptées depuis l'étranger font l'objet d'un rapide développement dans le rapport annuel 2014 du Conseil d'État :

> *« Le fait que les garanties entourant l'interception des communications soient moindres lorsqu'elles se situent à l'étranger plutôt que sur le territoire se justifie, bien qu'il fasse aujourd'hui l'objet de controverses. La différenciation de même nature (même si elle se fonde davantage sur la nationalité des personnes concernées) à laquelle procède la législation américaine a été l'un des points les plus critiqués à la suite des révélations de l'affaire PRISM, même si cet aspect n'était en rien secret ; elle fait en particulier l'objet d'une dénonciation virulente du Parlement européen dans sa résolution du 12 mars 2014. Pourtant, dès lors que les personnes situées à l'étranger échappent à la juridiction de l'État, l'interception de leurs communications n'est pas susceptible de porter atteinte à leurs droits dans la même mesure que si elles se situaient sur le territoire ; elles ne peuvent en particulier faire l'objet de mesures juridiques contraignantes qui se fonderaient sur les éléments collectés ».*

Avant même de rentrer dans une discussion juridique sur la constitutionnalité et la conventionnalité de l'article L. 854-1 et de critiquer la lecture partiale que fait le rapport du Conseil d'État du droit international et de la jurisprudence afférente –, il convient

7. Jacques Follorou, « La France, précieux partenaire de l'espionnage de la NSA », *Le Monde*, 29 novembre 2013. Disponible à l'adresse : `http://www.lemonde.fr/technologies/article/2013/11/29/la-france-precieux-partenaire-de-l-espionnage-de-la-nsa_3522653_651865.html`.

d'ajouter que cette distinction national/international était auparavant justifiée par les obstacles techniques qui limitaient fortement la capacité de l'État à conduire des opérations de surveillance hors des frontières et qui imposaient en pratique de se limiter à quelques cibles les plus stratégiques. Le renseignement restait dominé par des problématiques d'espionnage et de contre-espionnage. À cet égard, les récentes révélations de la presse sur la surveillance des chefs d'État et autres dirigeants français par la NSA ne constituent que le prolongement de pratiques somme toute anciennes [8].

Or, les limites techniques et doctrinales à la surveillance sont largement mises en cause par l'évolution des techniques numériques de communication et de usages :

- d'une part en raison de la puissance des outils informatiques utilisés pour la captation, le stockage ou l'analyse du trafic, qui permettent des économies d'échelle considérables ;
- de l'autre, en raison de la transnationalisation croissante des réseaux de communication, qui fait que même des communications purement nationales dans les décisions d'émission et de reception peuvent être « internationales » au plan technique, car transmises au travers d'équipements situés hors des frontières nationales ».

Du fait de ces évolutions, l'État est donc désormais en mesure d'intercepter et d'exploiter massivement et légalement les communications internationales. S'ajoutent à ces aspects techniques :

- l'évolution des doctrines dans le champ du renseignement, qui depuis 2001 a conduit à placer sous surveillance étendue des populations civiles ;
- le fait que s'est développée en même temps la coopération transnationale entre les services de renseignement de différents pays soumis à des régimes juridiques différents et s'échangeant des données hors de tout véritable contrôle.

L'ensemble de ces éléments remettent radicalement en cause la distinction traditionnelle entre surveillances nationale et internationale. Ce sont justement ces évolutions qui sont au cœur des révélations permises par Edward Snowden [9]– qui justifient l'ampleur des controverses auxquelles le Conseil d'État fait référence.

En acceptant la mise en place du régime spécial prévu par l'article L. 854-1, le législateur a refusé d'en tirer les conséquences et a violé la Constitution et le droit international.

9.4.2. La Constitution et le droit international imposent de respecter l'universalité des droits

En droit,

En son article premier, la Constitution dispose :

« Les hommes naissent et demeurent libres et égaux en droits. Les distinctions sociales

8. Voir les révélations de WikiLeaks, Mediapart et Libération du 23 juin dernier :Lenaïg Bredoux, Mathieu Magnaudeix et Ellen Salvi. Espionnage : l'Elysée dénonce des « faits inacceptables », *Mediapart*, 24 juin 2015. Disponible à l'adresse : `https://www.mediapart.fr/journal/france/240615/espionnage-lelysee-denonce-des-faits-inacceptables`

9. Ces évolutions et leurs conséquences juridiques sont analysées plus en détail dans une étude internationale conduite en réaction aux premières révélations d'Edward Snowden sur les pratiques de la NSA : « Scope : Extra-territorial Application of Human Rights Treaties » in *Background and Supporting International Legal Analysis*. Disponible à l'adresse : `https://en.necessaryandproportionate.org/LegalAnalysis/scope-extra-territorial-application-human-rights-treaties`.

ne peuvent être fondées que sur l'utilité commune ».

Selon l'article 2 alinéa premier du Pacte international relatif aux droits civils et politiques :

> *« Les États parties au présent Pacte s'engagent à respecter et à garantir à tous les individus se trouvant sur leur territoire et relevant de leur compétence les droits reconnus dans le présent Pacte, sans distinction aucune, notamment de race, de couleur, de sexe, de langue, de religion, d'opinion politique ou de toute autre opinion, d'origine nationale ou sociale, de fortune, de naissance ou de toute autre situation ».*

Enfin l'article 1er de la Convention de sauvegarde des droits de l'Homme dispose :

> *« Les Hautes Parties contractantes reconnaissent à toute personne relevant de leur juridiction les droits et libertés définis au titre I de la présente Convention ».*

S'il existe des controverses sur la portée extraterritoriale de ces deux textes internationaux, leur applicabilité dans les cas de surveillance internationale des communications est aujourd'hui largement acceptée.

Ainsi, la Grande chambre de la CEDH a jugé que la Convention européenne pouvait s'appliquer aux requérants étrangers, lesquels avaient le droit de saisir la Cour en vue d'une application territoriale de la Convention [10]. Un principe que l'on retrouve dans la jurisprudence relative à l'article 8 s'agissant des activités de surveillance des communications [11].

Quant au Pacte international relatif aux droits civils et politiques, rappelons qu'il protège expressément le droit à la vie privée et la confidentialité des correspondances à l'article 17 :

> *« 1. Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation*
>
> *« 2. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ».*

Dans son Observation générale nº 16, le Comité des droits de l'homme des Nations Unies a souligné que le respect de l'article 17 du Pacte international relatif aux droits civils et politiques exigeait que l'intégrité et le caractère confidentiel de la correspondance soient garantis en droit et en fait. « La correspondance doit être remise au destinataire, sans interception, sans être ouverte, et sans qu'il en soit pris autrement connaissance » [12]

Or, le Pacte garantit l'universalité des droits dans son article 2 paragraphe 1 :

10. Voir CEDH, 7 juillet 2011, *Al-Skeini et autres c. Royaume-Uni*, nº 55721/07 ; CEDH, 30 juin 2005, *Bosphorus c. Irlande*, nº 45036/98

11. Voir CEDH, 1er juillet 2008, *Liberty et autres c. Royaume-Uni*, nº 58243/00 (violation du droit à la vie privée d'une ONG irlandaise non présente sur le territoire britannique) ; CEDH, 29 juin 2006, *Weber et Saravia c. Allemagne*, 29 juin 2006, nº 54934/00 (la Cour est disposée à admettre la requête de deux citoyens uruguayens contre les pratiques des services allemands, mais la rejette sur d'autres fondements ; voir §72)

12. CCPR/C/21/Rev.1/Add.13,§10.

> *« Les États parties au présent Pacte s'engagent à respecter et à garantir à tous les individus se trouvant sur leur territoire et relevant de leur compétence les droits reconnus dans le présent Pacte, sans distinction aucune, notamment de race, de couleur, de sexe, de langue, de religion, d'opinion politique ou de toute autre opinion, d'origine nationale ou sociale, de fortune, de naissance ou de toute autre situation. ».*

Dans son Observation générale n° 31, qu'aux termes de cet article, tout État partie doit respecter et garantir *à quiconque se trouve sous son pouvoir ou son contrôle effectif les droits reconnus dans le Pacte même s'il ne se trouve pas sur son territoire*[13]. Cela s'étend aux individus relevant de sa « compétence ».

Dans son rapport publié un an après le début des révélations d'Edward Snowden et consacré au « droit à la vie privée à l'ère du numérique », le Haut-Commissariat des Nations Unies aux droits de l'homme soulignait à propos de cette casuistique :

> *« Le Comité des droits de l'homme s'est appuyé sur le principe, énoncé même dans sa jurisprudence la plus ancienne, qu'un État ne peut pas se soustraire à ses obligations internationales en matière de droits de l'homme en prenant en dehors de son territoire des mesures qui lui seraient interdites « chez lui »*[14]*. Cette position est conforme aux vues de la Cour internationale de Justice qui a affirmé que le Pacte international relatif aux droits civils et politiques est applicable aux actes d'un État agissant « dans l'exercice de sa compétence en dehors de son propre territoire »*[15]*, ainsi qu'aux articles 31 et 32 de la Convention de Vienne sur le droit des traités. Les notions de « pouvoir » et de « contrôle effectif » permettent de reconnaître qu'un État exerce une « compétence » ou des pouvoirs publics, dont les mesures de protection des droits de l'homme sont destinées à freiner les abus.* Un État ne peut pas se soustraire à ses responsabilités en matière de droits de l'homme simplement en s'abstenant d'inscrire ces pouvoirs dans les limites de la loi. En tirant une autre conclusion, non seulement on affaiblirait l'universalité et l'essence des droits protégés par le droit international des droits de l'homme *mais l'on pourrait aussi inciter structurellement les États à se déléguer mutuellement les tâches de surveillance.*
>
> *34. Il s'ensuit que* la surveillance numérique peut donc mettre en cause les obligations d'un État en matière de droits de l'homme si elle fait intervenir l'exercice du pouvoir ou le contrôle effectif dudit État à l'échelle de l'infrastructure des communications numériques, où que cela se produise, par exemple sous la forme d'écoutes directes ou d'une pénétration de l'infrastructure en place. *De même, dans les cas où l'État exerce une compétence réglementaire sur une tierce partie qui contrôle physiquement les données, cet État aura aussi des obligations en vertu du Pacte. Si un pays souhaite établir sa compétence sur les données d'entreprises privées au motif que ces entreprises ont été constituées en société sur son territoire, alors les protections des droits de l'homme doivent s'étendre aux personnes victimes d'immixtions dans leur vie privée, que ce soit dans le pays où les sociétés ont été constituées ou ailleurs. Cela reste valable que l'exercice de cette compétence soit légal ou non à l'origine, ou viole de fait la souveraineté d'un autre État. »*

13. Documents officiels de l'Assemblée générale des Nations Unies, 36ème session, Supplément n° 40 (A/36/40), annexe XIX, §12.2.

14. Voir *Documents officiels de l'Assemblée générale, trente-sixième session*, (voir la note de bas de page 27), annexe XIX, par. 12.2 et 12.3, et annexe XX, par. 10.3.

15. Avis consultatif de la Cour internationale de Justice sur les *conséquences juridiques de l'édification d'un mur dans le territoire palestinien occupé*, du 9 juillet 2004 (A/ES-10/273 et Corr.1), par. 107 à 111. Voir aussi Cour internationale de Justice, *Activités armées sur le territoire du Congo (République démocratique du Congo c. Ouganda)*, arrêt, 2005, p. 168.

(Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme, « Le droit à la vie privée à l'ère du numérique », rapport n° HRC/27/37, Conseil des droits de l'Homme, Assemblée générale des Nations Unies, 27ème session, 30 juin 2014, §33)

En l'espèce,

Comme mentionné en introduction de cet examen, **la loi déférée n'apporte aucune garantie pour la surveillance des communications lorsqu'elle est conduite hors des frontières nationales ou pour la surveillance des communications émises *et* reçues à l'étranger**. Outre ce que cela se déduit de l'absence de toute disposition explicite pour ce type de mesure (cf *supra* 9 page 69), la loi crée par son article 10 un article 323-8 dans le code pénal qui accorde une immunité aux agents des services de renseignement contre toute poursuite pénale en lien avec la criminalité informatique dès lors qu'il s'agit d'assurer leurs missions « hors du territoire national » (intrusion, captation, destruction d'équipements informatiques, notamment) [16]. Du fait de cette absence d'encadrement des opérations conduites au-delà des frontières, **les expatriés français ne disposeront d'aucune protection**. Entre 1,5 et 2 millions de citoyens français sont directement concernés [17].

S'agissant de la surveillance des communications émises ou reçues à l'étranger qui ne sont pas rattachables au territoire national, lorsqu'elle est conduite en tout ou en partie sur le territoire national (régie par l'article L. 854-1), les autorisations du Premier ministre (définies au I de l'article attaqué suite à un amendement sénatorial) ne revêtent aucun caractère individuel et autorisent dès lors des interceptions indiscriminées de correspondances et autres communications :

> *« Les autorisations de surveillance des communications concernées et les autorisations d'exploitation ultérieure des correspondances désignent les systèmes de communication, les zones géographiques, les organisations ou les personnes ou groupes de personnes objets de la surveillance, la ou les finalités justifiant cette surveillance ainsi que le ou les services spécialisés de renseignement qui en sont chargés ».*

Ce type d'autorisation sans mandat individuel rappelle là encore les procédures à l'œuvre aux États-Unis, telles qu'elles résultent de la section 702 du Foreign Intelligence Surveillance Act (FISA).

En conclusion,

En renonçant à toute forme d'encadrement législatif dès lors que les communications sont interceptées et exploitées hors des frontières nationales ou lorsque les communications sont émises *et* reçues à l'étranger ;
en échouant à apporter des garanties adéquates et effectives pour les personnes dont les communications sont émises ou reçues à l'étranger ;

16. L'article 323-8 dispose : « le présent chapitre n'est pas applicable aux mesures mises en œuvre, par les agents habilités des services de l'État désignés par arrêté du Premier ministre parmi les services spécialisés de renseignement mentionnés à l'article L. 811-2 du code de la sécurité intérieure, pour assurer hors du territoire national la protection des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du même code ».

17. Le ministère des Affaires étrangères fait état de 1 611 054 d'inscrits au Registre mondial des Français établis hors de France au 31 décembre 2012 et précise qu'il faudrait sans doute ajouter environ 500 000 français non-inscrits, en raison du caractère non obligatoire de cette inscription.

le législateur a violé l'article premier de la Déclaration des droits de l'Homme et du citoyen et l'article 34 de la Constitution, et a méconnu tant la CESDH que le Pacte international relatif aux droits civils et politiques.

Partant, l'ensemble de l'article L. 854-1 à l'exception de la première phrase [18] et d'une partie de la première phrase du II [19], doit être censuré.

18. La première phrase contient les mots : « Le Premier ministre, ou l'une des personnes déléguées mentionnées à l'article L. 821-4, peut autoriser, aux seules fins de protection des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3, la surveillance [...] des communications qui sont émises ou reçues à l'étranger ».

19. Les mots : « celles-ci sont exploitées dans les conditions prévues au même article L. 852-1 et conservées et détruites dans les conditions prévues aux articles L. 822-2 à L. 822-4, sous le contrôle de la Commission nationale de contrôle des techniques de renseignement »

Quatrième partie

CONTRÔLES DES TECHNIQUES

10. Contrôle préalable

Par les dispositions du code de la sécurité intérieure édictées par la présente loi, le législateur entend donner un cadre juridique aux activités des services de renseignement. Or, en ne soumettant pas l'activité de ces services au contrôle préalable d'une juridiction, il a échoué à prévoir la garantie exigée par la Constitution (section 10.1 page suivante) pour assurer l'équilibre nécessaire entre les atteintes aux droits et libertés fondamentaux qu'il autorise (section 10.2 page 89) et les objectifs qu'il poursuit [1].

À cela s'ajoutent des imprécisions affectant le contrôle des autorisations des mesures de renseignement (section 10.3 page 96) et l'insuffisance des garanties apportées aux professions dont le secret est protégé (section 10.4 page 99).

À titre préliminaire, deux remarques s'imposent.

Premièrement, comme cela a déjà été relevé (chapitre 3 page 15), les moyens mis en œuvre par la présente loi sont en décalage complet avec les objectifs qu'elle vise. Non seulement la mise en place de procédés de renseignement ne saurait être justifiée pour l'ensemble des comportements visés mais, qui plus est, l'accomplissement de certains objectifs visés par le législateur ne nécessite en aucune manière l'absence de contrôle juridictionnel *a priori*.

Deuxièmement, il est à reconnaître qu'en s'engageant sur la voie d'un contrôle juridictionnel seulement *a posteriori* et qui plus est on ne peut plus lacunaire par le Conseil d'État (voir *infra*, chapitre 11.3 page 114), la France est particulièrement isolée au sein des démocraties modernes. Comme le relevait le Conseil d'État dans son étude annuelle pour l'année 2014, les États-Unis ont par exemple institué une cour spécialisée et habilitée secret défense permettant d'assurer un contrôle extérieur à l'administration sur les mesures mises en place par elle. Le fait que cette Cour n'ait pas empêché la collecte illicite de données par la NSA, reconnue comme telle par une Cour fédérale des États-Unis, ne doit pas conduire à la conclusion que l'intervention d'une juridiction *a priori* ne permettrait pas d'assurer la garantie des droits. Si le système mis en place aux États-Unis s'est montré défaillant, c'est notamment en ce que les termes de la loi elle-même ont institué un contrôle lacunaire, incompatible avec les garanties élémentaires du droit au procès équitable, prévoyant des dérogations au droit commun excédant largement la stricte nécessité liée au secret de la défense nationale [2].

1. Pour rappel, l'absence de contrôle préalable des mesures de surveillance internationale fait l'objet de développements à la section 9.3.2 page 74.

2. Voir les problèmes similaires posés par la procédure contentieuse créée par la présente loi, chapitre 11.3 page 114.

La conclusion qu'il faut tirer de cette expérience étrangère est que les techniques de renseignement doivent être soumises à un contrôle dont la portée est effective. Cette effectivité peut être garantie, par exemple, en permettant un accès au dossier dans son intégralité, en permettant de procéder à une analyse fine des matériels sollicités, en empêchant les collectes de masse, en permettant au juge de déclassifier de son propre chef certaines pièces, notamment. Dans tous les cas, cette effectivité dépend avant toute chose de la soumission des mesures de surveillance à un contrôle juridictionnel préalable.

10.1. L'exigence constitutionnelle d'un contrôle juridictionnel préalable

Le respect des droits et libertés reconnus par la Déclaration de 1789 et les exigences posées par l'article 34 de la Constitution impliquent pour le législateur l'obligation de prévoir les « garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques » parmi lesquelles figurent le respect de la vie privée et la liberté d'expression et de communication, respectivement protégés par les articles 2 et 11 de la Déclaration de 1789.

Ainsi, la protection de ces droits reconnus aux citoyens contre des atteintes d'une gravité particulière implique de requérir l'intervention et le contrôle d'une autorité juridictionnelle, que ce soit ceux de *l'autorité judiciaire*, gardienne de la liberté individuelle (section 10.1.1) ou, à tout le moins, ceux d'une *juridiction* offrant les garanties d'indépendance et d'effectivité nécessaires, en cas d'atteinte aux droits et libertés fondamentaux (section 10.1.2 page suivante).

10.1.1. L'exigence d'un contrôle préalable de l'autorité judiciaire sur les atteintes à la liberté individuelle

L'article 66 de la Constitution dispose que :

> *Nul ne peut être arbitrairement détenu.*
>
> *L'autorité judiciaire, gardienne de la liberté individuelle, assure le respect de ce principe dans les conditions prévues par la loi.*

Le Conseil constitutionnel a déjà considéré :

> *que la méconnaissance du droit au respect de la vie privée* ***peut*** *être de nature à* ***porter atteinte à la liberté individuelle****.*
>
> (Décision n° 94-352 DC du 18 janvier 1995)

Certes, les associations *amicus* n'ignorent pas que la notion de liberté individuelle est distincte de la notion de liberté personnelle, reconnue à l'article 2 de la Déclaration de 1789, laquelle implique le droit au respect de la vie privée (Cons. constit. Dec. n° 99-416 DC du 23 juillet 1999, cons. 45), mais aussi le droit à la sûreté et à la résistance à l'oppression.

Pour autant, le contrôle de l'autorité judiciaire a vocation à s'appliquer pour prévenir des atteintes arbitraires au droit au respect de la vie privée, lorsque ces atteintes sont tellement graves qu'elles peuvent avoir pour effet de porter atteinte à la liberté individuelle.

Il en est de même en cas d'atteinte grave à la sûreté des personnes, puisque l'autorité judiciaire est aussi garante du principe que nul ne peut être arbitrairement détenu.

Aucune règle constitutionnelle n'implique de distinction *exclusive* entre la protection de la liberté personnelle et la nécessité de requérir l'intervention de l'autorité judiciaire, gardienne de la liberté individuelle. À ce sujet, le professeur Vincent Mazeaud écrivait récemment en ce sens :

> « *Cela ne signifie pas pour autant que l'article 66 soit mécaniquement exclu en présence d'une atteinte à la vie privée : ces deux articles [2 et 66] peuvent évidemment faire l'objet d'une application combinée.* »
>
> (V. Mazeaud, La constitutionnalisation du droit au respect de la vie privée, Nouveaux Cahiers du Conseil constitutionnel, 1er juin 2015, nº 48, p. 7)

À l'inverse, **une mesure susceptible de porter une atteinte particulièrement grave au respect au droit à la vie privée peut être de nature à porter atteinte à la liberté individuelle** ; dans ce cas, une telle mesure exige qu'elle relève du monopole de l'autorité judiciaire — de la même façon que les atteintes particulièrement graves au droit à la sûreté relèvent de l'autorité judiciaire.

Ainsi, en matière de procédure pénale, le Conseil constitutionnel assure le respect de la liberté individuelle en imposant que les garanties entourant des mesures portant atteinte à la vie privée répondent aux exigences constitutionnelles de l'article 66 et qu'en outre ces mesures soient proportionnées au but poursuivi par le législateur, ce qui implique des *garanties procédurales appropriées*. De sorte, il a pu juger que, « eu égard aux exigences de l'ordre public et de la poursuite des auteurs d'infractions, le législateur peut prévoir la possibilité d'opérer des perquisitions, visites domiciliaires et saisies de nuit dans le cas où un crime ou un délit relevant de la criminalité et de la délinquance organisées vient de se commettre, **à condition que l'autorisation de procéder à ces 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 nº 2004-492 DC du 2 mars 2004, cons. 46).

10.1.2. L'exigence d'un contrôle préalable d'une autorité juridictionnelle sur les atteintes graves aux droits et libertés

Même en l'absence d'une atteinte à la liberté individuelle et au regard du seul article 34 de la Constitution, le Conseil constitutionnel a déjà pu exiger le contrôle d'une autorité juridictionnelle destiné à assurer une conciliation équilibrée et proportionnée entre les buts poursuivis par le législateur et les exigences de protection des droits et libertés consacrés par la Déclaration de 1789.

De jurisprudence constante, la Cour EDH considère elle aussi qu'une société démocratique « *implique, entre autres, qu'une ingérence de l'exécutif dans les droits d'un individu soit soumise à un contrôle efficace* » et que ce contrôle doit normalement être assuré par « *le pouvoir judiciaire* car il offre les meilleures garanties d'indépendance, d'impartialité et de procédure régulière » (CEDH, *Klass et autres c. Allemagne*, 6 septembre 1978, nº 5029/71, §55).

10.1.2.1. Sur les atteintes au droit au respect de la vie privée

Ainsi, l'existence d'un contrôle judiciaire permanent sur les actions des autorités administratives a été fréquemment regardée par le Conseil constitutionnel comme l'une des garanties de la proportionnalité de l'atteinte portée à la vie privée. Tel fut le cas concernant les dispositions relatives au fichier des auteurs d'infractions sexuelles consultable par l'administration,à propos desquelles le Conseil a jugé que :

> *« 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. constit., Dec. n° 2004-492 DC du 2 mars 2004, cons. 87).

Il en fut de même concernant les dispositions relatives aux interceptions de correspondances électroniques réalisées lors de l'instruction pénale :

> *« Les dispositions critiquées ne s'appliquent que pour la recherche des auteurs des infractions entrant dans le champ d'application de l'article 706-73 ;* ***qu'elles doivent être exigées par les besoins de l'enquête et autorisées par le juge des libertés et de la détention*** *du tribunal de grande instance, à la requête du procureur de la République ; [...] dans ces conditions, les dispositions critiquées ne portent une atteinte excessive ni au secret de la vie privée ni à aucun autre principe constitutionnel ; »*
>
> (Cons. constit., Dec. n° 2004-492 DC du 2 mars 2004, cons. 59 à 61).

En d'autres termes, **une mesure susceptible d'emporter une atteinte particulièrement grave au respect au droit à la vie privée peut exiger, afin de satisfaire à l'exigence constitutionnelle de proportionnalité, qu'elle soit placée sous le contrôle d'une juridiction**.

10.1.2.2. Sur les atteintes à la liberté d'expression et de communication

Ensuite, au titre de la liberté d'expression et de communication, le Conseil constitutionnel a 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 — qui n'est pas une juridiction, même si celle-ci était une autorité administrative 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. constit., Déc. n° 2009-580 DC du 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 permettre de telles mesures.

Il est d'ailleurs particulièrement révélateur que, dans cette décision du 10 juin 2009, le Conseil constitutionnel a 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 confié à une autorité administrative en lieu et place d'une juridiction et que « la totalité de la population » soit potentiellement visée.

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.

En conclusion,

Au regard tant de l'article 34 que de l'article 66 de la Constitution, il faut nécessairement l'autorisation d'une juridiction pour la garantie effective du respect des droits et libertés fondamentaux auxquels une loi porte atteinte, dès l'instant où l'atteinte qui leur est faite présente une particulière gravité : soit parce qu'elle porte atteinte à la liberté individuelle, soit parce que les mesures concernées ne visent pas une catégorie de personnes mais bien la totalité de la population.

10.2. L'absence injustifiable de contrôle juridictionnel préalable des atteintes particulièrement graves portées aux libertés

Le défaut de contrôle juridictionnel préalable de la mise en œuvre des techniques de renseignement est manifestement injustifié au regard de la gravité des atteintes que cette mise en œuvre porte aux droits et libertés garantis (sous-section 10.2.1), de l'ineffectivité du contrôle administratif prévu par la présente loi (sous-section 10.2.2 page 93) et de ce que le Conseil constitutionnel exige une autorisation judiciaire dans des cas analogues (sous-section 10.2.3 page 94).

10.2.1. Des atteintes d'une particulière gravité au droit à la vie privée et à la liberté de communication ainsi qu'à la liberté individuelle

Les mesures en cause sont en effet d'une gravité inédite. Il s'agit notamment d'autoriser les services de renseignement à entrer dans les foyers, dans les véhicules, dans les

lieux de vie pour les sonoriser, pour y prélever les renseignements qu'eux seuls jugeront utiles, d'écouter les conversations entre des personnes suspectées, mais aussi d'analyser en temps réel les communications *via* le recueil d'informations ou de documents concernant des personnes contre lesquelles il n'existe aucune suspicion d'un lien direct ou même lointain avec une infraction.

Ces mesures n'emportent pas seulement une soustraction pure et simple du droit à la vie privée des personnes mises en cause directement ou indirectement par ces mesures (section 10.2.1.1), mais également une atteinte aux libertés de ces personnes. En effet, ces mesures portent atteinte à la liberté de communication de l'ensemble de la population (section 10.2.1.2 page ci-contre), ainsi qu'à la liberté individuelle des personnes ciblées (section 10.2.1.3 page suivante).

10.2.1.1. Des atteintes au droit à la vie privée

Plusieurs techniques de renseignement permettent de porter atteinte au droit au respect de la vie privée de la totalité de la population. En effet, la présente loi autorise l'accès à tout « information ou document » conservé ou traité par les réseaux d'opérateurs ou les services de prestataires par lesquels sont traitées les communications électroniques **de la totalité de la population**.

Ainsi, l'article 2 de la loi crée un titre V, chapitre I^{er} « Des accès administratifs aux données de connexion ». Ces données peuvent être requises administrativement sur demande ou en temps réel (L. 851-1 et -2) ou faire l'objet d'une analyse automatique par la mise en œuvre de traitements algorithmiques automatisés (L. 851-3). Or, comme démontré *supra* (section 5.2.4 page 41), ces données sont de nature à révéler des informations très précises et structurées sur toutes les personnes qui en sont l'objet — y accéder constitue donc *a fortiori* une ingérence d'une vaste ampleur et d'une gravité particulière.

Par conséquent, ces mesures confèrent aux services de renseignement un pouvoir démesuré pouvant conduire à restreindre le respect de la vie privée de la totalité de la population, c'est-à-dire la possibilité pour tout un chacun de se voir préservé dans son intimité pour l'exercice de sa liberté personnelle garantie par l'article 2 de la Déclaration de 1789. Eu égard à la nature du droit au respect de la vie privée, de telles mesures ne sauraient être assorties de garanties efficaces en dehors d'un contrôle juridictionnel.

Ces atteintes, ainsi que les atteintes portées par les techniques de captation, sont d'autant plus disproportionnées qu'elles sont autorisées pour la poursuite de finalités non définies ou excessives, telle que la promotion des « intérêts économiques, industriels et scientifiques majeurs de la France » ou la prévention de l'emploi personnel de stupéfiants (voir chapitre 3 page 15). Il semble dès lors incohérent que la poursuite de telles finalités, portant de telles atteintes, puisse échapper à tout contrôle juridictionnel préalable alors même que le Conseil constitutionnel soumet à un tel contrôle la recherche et la constatation des crimes les plus graves par la police judiciaire (voir section 10.2.3 page 94)

Par ailleurs, les atteintes spéciales contre la pratique du chiffrement des communications constituent une ingérence à la fois dans le droit au respect de la vie privée et dans le droit de résister à l'oppression, tous deux reconnus à l'article 2 de la Déclaration de 1789 (chapitre 6 page 47).

10.2.1.2. Des atteintes à la liberté de communication

Les techniques de renseignement autorisées par la présente loi emportent aussi une atteinte à la liberté de communication de l'ensemble de la population dont la gravité et la réalité sont à reconnaître. Il est en effet désormais très largement établi que la mise en place de dispositifs de surveillance porte une atteinte à la liberté de communication non seulement des personnes qui en font l'objet mais aussi des personnes qui, alors même qu'elles ne sont pas susceptibles d'être légitimement surveillées par des services de renseignement, s'autocensurent, changent leur mode d'expression ainsi que leurs habitudes d'utilisation des techniques de communication et plus grave encore se restreignent dans leur recherche d'informations [3].

C'est ce lien direct entre la surveillance d'une part et les libertés d'opinion et de communication d'autre part qui est mis en évidence par la CEDH dans son arrêt *Klass et autres c. Allemagne* de 1978 :

> *« (...) la législation elle-même crée par sa simple existence, pour tous ceux auxquels on pourrait l'appliquer, une menace de surveillance entravant forcément la liberté de communication entre usagers des services des postes et télécommunications et constituant par là une « ingérence d'une autorité publique » dans l'exercice du droit des requérants au respect de leur vie privée et familiale ainsi que de leur correspondance. »*
>
> En l'espèce, les requérants n'avaient pas été effectivement surveillés, mais leur requête fut acceptée car ils étaient tout de même victimes de l'ingérence.
>
> (CEDH, *Klass et autres c. Allemagne*, 6 septembre 1978, n° 5029/71, §41)

Par conséquent, et outre l'atteinte à la vie privée, ces mesures confèrent aux services de renseignement un pouvoir démesuré pouvant conduire à restreindre l'exercice, par toute personne, de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile — ce que garantit l'article 11 de la Déclaration de 1789. Eu égard à la nature de cette liberté, de telles mesures ne sauraient être assorties de garanties efficaces en dehors d'un contrôle juridictionnel.

10.2.1.3. Des atteintes à la liberté individuelle

Enfin, la mise en œuvre de certaines techniques de surveillance relève d'une intrusion d'une gravité sans précédent. Une surveillance quasi totale d'une personne, telle que les mesures de renseignement autorisées le permettent, est de nature à porter atteinte à la liberté individuelle des personnes ciblées.

À l'instar des procédures dérogatoires de la procédure pénale, les techniques de captation, de fixation, de transmission et d'enregistrement de paroles prononcées à titre privé

3. Voir à ce sujet deux études récentes :

1. Lee Rainie et Mary Madden. Americans' Privacy Strategies Post-Snowden, *Pew Research Center's Internet & American Life Project*, 16 mars 2015. Disponible à l'adresse : `http://www.pewinternet.org/2015/03/16/Americans-Privacy-Strategies-Post-Snowden/` et
2. Chris Chambers. The psychology of mass government surveillance, *The Guardian*, 18 mars 2015. Disponible à l'adresse : `http://www.theguardian.com/science/head-quarters/2015/mar/18/the-psychology-of-mass-government-surveillance-how-do-the-public-respond-and-is-it-changing-our-behaviour`.

ou confidentiel ou d'images dans un lieu privé institué par l'article 3 de la loi déférée à l'article L. 853-1 du CSI relèvent d'un caractère suffisamment grave puisque de tels moyens ne peuvent être mis en œuvre que lorsque les renseignements recueillis ne peuvent l'être par un autre moyen légalement autorisé moins attentatoire. En effet, un tel degré de surveillance et d'intrusion constant relève en réalité d'une atteinte à la liberté individuelle même des personnes qui en font l'objet.

Il en va exactement de même pour les techniques de captation de données informatiques prévues à l'article L. 853-2, qui ont pour effet de priver, à leur insu, les personnes concernées de la pleine maîtrise de leurs équipements informatiques personnels (voir chapitre 8 page 63), alors que ces outils ainsi que toutes les données qu'ils contiennent permettent de manière exhaustive et intrusive comme jamais auparavant de s'immiscer dans la sphère individuelle intime de la personne.

Nous relevons à ce sujet que M. le député Jean-Jacques Urvoas relève lui-même qu'il s'agit d'**atteintes à la liberté individuelle**[4] :

> **M. Jean-Jacques Urvoas,** *député, rapporteur pour l'Assemblée nationale.* - Ma proposition de rédaction ne soulève aucun problème de constitutionnalité[5]. Les jurisprudences du Conseil constitutionnel et de la Cour européenne des droits de l'homme reconnaissent toutes deux la possibilité de déroger au principe d'égalité, y compris lorsqu'**il s'agit de porter atteinte à l'exercice d'une liberté individuelle**, si cette atteinte n'est pas excessive. [...]

Bien que les associations *amicus* ne partagent pas l'analyse qui est faite de l'application de la jurisprudence du Conseil aux dispositions en cause (les dispositions relatives à l'autorisation des techniques décrites au titre V du code de la sécurité intérieure créé par la loi déférée), elles s'accordent avec M. Urvoas, maître de conférence en droit public et président de la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République de l'Assemblée nationale, et auteur d'un rapport parlementaire inédit sur les activités des services de renseignement[6], pour dire qu'il s'agit d'atteintes à la liberté individuelle.

En conclusion,

Compte tenu de la gravité et de la multiplicité des atteintes aux droits qui résulteraient de la mise en œuvre des techniques de renseignement en cause en l'espèce, leur proportionnalité ne peut être assurée que dans la mesure où l'équilibre des pouvoirs est garanti, quels que soient les objectifs annoncés par le législateur.

---

4. Texte repris du compte rendu intégral des débats tel que diffusé par le site web du Sénat à l'adresse : `http://www.senat.fr/compte-rendu-commissions/20150615/cmp.html`

5. Note : il s'agit de l'ajout à l'article L. 821-1 de l'alinéa 2 : « Par dérogation au premier alinéa, lorsque la mise en œuvre sur le territoire national d'une technique de renseignement ne concerne pas un Français ou une personne résidant habituellement sur le territoire français, l'autorisation est délivrée par le Premier ministre sans avis préalable de la Commission nationale de contrôle des techniques de renseignement. »

6. *Rapport d'information en conclusion des travaux d'une mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, enregistré à la Présidence de l'Assemblée Nationale, le 14 mai 2013, disponible à l'adresse : `http://www.assemblee-nationale.fr/14/pdf/rap-info/i1022.pdf`

10.2.2. L'ineffectivité du contrôle administratif préalable prévu

La présente loi soumet la mise en œuvre des techniques qu'elle institue à l'autorisation du Premier ministre, prévue à l'article L. 821-1, ainsi qu'à l'avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR), prévue à l'article L. 821-3.

Or, la seule autorisation du Premier ministre ne saurait offrir la moindre garantie contre l'arbitraire, ce dernier partageant avec le Président de la République l'autorité directe sur les services de renseignement. Ainsi, le contrôle de la CNCTR est la seule garantie proposée par la loi pour assurer le respect des droits et libertés mis en cause. Or, un tel contrôle apparaît comme manifestement inefficace à chacune des étapes auxquelles il intervient.

10.2.2.1. Le caractère consultatif des avis délivrés par la CNCTR

Premièrement, contrairement aux autorisations requises du juge judiciaire par la police judiciaire pour porter atteinte à la vie privée[7], les décisions de la CNCTR sont **de simples avis consultatifs** ne conditionnant nullement la mise en œuvre des techniques de renseignement.

De même, la CNCTR ne dispose d'aucun pouvoir contraignant lorsqu'elle constate qu'une technique va être mise en œuvre en violation de la présente loi. Elle ne peut que produire des recommandations au Premier ministre ou, à terme, saisir le Conseil d'État, dans des conditions portant une atteinte injustifiée aux droits et libertés.

10.2.2.2. Le caractère facultatif des avis délivrés par la CNCTR

Deuxièmement, la présente loi ne prévoit pas que tel avis soit systématiquement rendu. En effet, alors que l'article L. 821-1 prévoit que l'autorisation du Premier ministre est par principe « délivrée après avis de la Commission nationale de contrôle des techniques de renseignement », l'article L. 821-3 prévoit, à son second alinéa, que « en l'absence d'avis transmis dans les délais prévus au même article, celui-ci est réputé rendu », ces délais étant de 24h lorsque la demande d'autorisation n'est examinée que par le seul membre de la CNCTR à qui elle a été transmise, et de 72h lorsqu'elle est examinée par la formation restreinte ou plénière de la CNCTR.

Ainsi, dès l'instant où les services transmettraient simultanément un nombre de demandes trop important pour que la CNCTR puisse les examiner en 24h par un de ses membres ou en 72h par au moins trois de membres, une part potentiellement importante de ces demandes serait autorisée sans qu'aucun avis n'ait été rendu quant à leur conformité à la présente loi. Dès lors, les services de renseignement disposent de moyens pratiques sérieux pour affaiblir l'effectivité du contrôle auquel leurs activités sont soumises.

7. Voir sous-section 10.2.3 page suivante

10.2.2.3. Le contournement de l'avis préalable de la CNCTR au moyen des procédures d'urgence

Troisièmement, la présente loi ne prévoit pas davantage que tel avis soit systématiquement rendu au préalable de la mise en œuvre des techniques. En effet, l'article L. 821-5 prévoit que « en cas d'urgence absolue et pour les seules finalités mentionnées aux 1° et 4° 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. ».

Plus nettement encore, l'article L. 821-6 prévoit que « en cas d'urgence liée à une menace imminente ou à un risque très élevé de ne pouvoir effectuer l'opération ultérieurement, les appareils ou dispositifs techniques mentionnés aux articles L. 851-5 et L. 851-6 peuvent, de manière exceptionnelle, être installés, utilisés et exploités sans l'autorisation préalable mentionnée à l'article L. 821-4 par des agents individuellement désignés et habilités ». Les dispositifs ici visés sont ceux permettant la localisation en temps réel d'une personne, d'un véhicule ou d'un objet ou le recueil de données techniques de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ainsi que les données relatives à la localisation des équipements terminaux utilisés.

Dans ces deux cas — l'urgence « absolue » ou l'urgence « opérationnelle » —, les conditions permettant de différer l'avis de la CNCTR sont arbitrairement établies par les personnes s'en prévalant, à savoir le Premier ministre et les agents concernés.

En conclusion,

Le contrôle préalable prévu par la présente loi, qui n'est que consultatif et facultatif, échoue manifestement à offrir les garanties fondamentales exigées par la Constitution et par le droit international pour assurer le respect des droits et libertés protégés par cette dernière, alors même que les techniques en cause portent des atteintes d'une particulière gravité au droit à la vie privée et à la liberté de communication ainsi qu'à la liberté individuelle.

10.2.3. L'incohérence de l'absence de contrôle juridictionnel préalable

Le Conseil constitutionnel considère l'*autorisation préalable d'une juridiction* comme une garantie nécessaire au respect de droits et libertés fondamentaux lorsque la police judiciaire met en œuvre des techniques d'interception de correspondances [8], de captation

8. Cons. const., décision 2004-492 DC, 2 mars 2004, cons. 59 à 61 : « Considérant que les dispositions critiquées ne s'appliquent que pour la recherche des auteurs des infractions entrant dans le champ d'application de l'article 706-73 ; qu'elles doivent être exigées par les besoins de l'enquête et autorisées par le juge des libertés et de la détention du tribunal de grande instance, à la requête du procureur de la République ; 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 ; Considérant, par ailleurs, que demeurent applicables les garanties procédurales requises pour l'utilisation de tels procédés dans le cadre de l'instruction, s'agissant des autres types d'infractions ; Considérant que, dans ces conditions, les dispositions critiquées ne portent une atteinte excessive ni au secret de la vie privée ni à aucun autre

de paroles et d'images privées [9] ou de géolocalisation [10] ou porte atteinte à l'inviolabilité du domicile [11], alors que ces mesures correspondent respectivement à celles prévues aux articles L. 852-1, L. 853-1, L. 851-5 et L. 853-3 de la présente loi et que les services de renseignement peuvent mettre en œuvre sans l'autorisation préalable d'une juridiction.

Or, cette différence de garantie ne saurait être justifiée de ce que seule la police judiciaire a pour mission de participer à la répression des infractions, contrairement aux services de renseignement, car ces services y participent en vérité aussi, en application de l'article 40 du code de procédure pénale auquel renvoie l'article L. 811-2 de la présente loi et qui dispose, à son second alinéa, que :

> *« Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs. »*

Ensuite, cette différence de garantie ne saurait être non plus justifiée de ce que la police judiciaire poursuit des objectifs moins impérieux, urgents ou complexes que les services de renseignement, ou de ce qu'elle porte ce faisant des atteintes plus importantes aux droits et libertés garantis — au contraire.

En effet, la police judiciaire ne recherche que les auteurs d'infractions, alors que les services de renseignement peuvent surveiller toute personne dont le comportement ne viole aucune loi mais pourrait simplement nuire à la promotion d'un des nombreux intérêts fondamentaux visés par la présente loi — tels que des intérêts économiques. De plus, la police judiciaire ne recherche que des faits concrets — des infractions déjà réalisées, imminentes ou en cours —, alors que la police administrative recherche de simples faits potentiels, représentant un risque bien plus hypothétique pour l'ordre public et la Nation.

Par ailleurs, la police judiciaire et les services de renseignement peuvent rechercher des faits qu'il s'agit de prévenir avec la même urgence : pour l'enquête judiciaire, lorsqu'il s'agit par exemple d'interpeller l'auteur d'un crime contre les personnes avant qu'il ne puisse réitérer son acte, ou de retrouver une personne enlevée, ou, pour l'enquête administrative, lorsqu'il s'agit de prévenir un attentat probable. De même, les deux types d'investigations peuvent connaître la même exigence du secret, la police judiciaire s'en étant toujours accommodée.

Ainsi, rien ne distingue un type d'investigation par rapport à l'autre, si ce n'est que les dangers que peut prévenir la police judiciaire, dans sa mission de répression, sont

---

principe constitutionnel ; »

9. Cons. const., décision 2004-492 DC, 2 mars 2004, cons. 64 à 66 : « la mise en place de dispositifs techniques ayant pour objet, sans le consentement des intéressés, la captation, la fixation, la transmission et l'enregistrement de paroles ou d'images » est conforme à la Constitution dès lors, notamment, que « l'autorisation de les utiliser émane de l'autorité judiciaire »

10. Cons. const., décision 2014-693 DC, 25 mars 2014 ; cons. 17 : « le législateur a entouré la mise en œuvre de la géolocalisation de mesures de nature à garantir que, placées sous l'autorisation et le contrôle de l'autorité judiciaire, les restrictions apportées aux droits constitutionnellement garantis soient nécessaires à la manifestation de la vérité et ne revêtent pas un caractère disproportionné au regard de la gravité et de la complexité des infractions commises ; »

11. Cons. const., décision 2004-492 DC, 2 mars 2004, cons. 46 : « le législateur peut prévoir la possibilité d'opérer des perquisitions, visites domiciliaires et saisies de nuit dans le cas où un crime ou un délit relevant de la criminalité et de la délinquance organisées vient de se commettre, à condition que l'autorisation de procéder à ces opérations émane de l'autorité judiciaire »

imminents ou en cours et constituant systématiquement des infractions, quand ceux que peuvent prévenir les services de renseignement sont en principe potentiels et peuvent viser des comportements parfaitement licites. *De facto*, les recherches conduites par les services de renseignement portent atteinte, par leur nature, à la vie privée d'un nombre bien plus important de personnes qui se révéleront à terme n'avoir finalement fait naître aucun risque pour les intérêts de la Nation.

Il serait dès lors absurde de refuser de placer les renseignements administratifs sous le même contrôle judiciaire auquel le Conseil constitutionnel soumet un type d'investigation plus immédiat et portant une atteinte plus limitée aux droits et libertés fondamentaux de la population. En témoigne le fait que la loi déférée n'exige pas l'autorisation préalable d'un juge pour que des services de renseignement puissent géolocaliser un individu susceptible de cultiver du cannabis (voir chapitre 3 page 15), alors que le Conseil constitutionnel a exigé, de par sa jurisprudence, qu'un juge ait au préalable autorisé la police judiciaire pour que celle-ci puisse géolocaliser les auteurs des attentats terroristes de janvier dernier, alors même que ceux-ci venaient de commettre leurs premiers crimes, dont la réitération semblait certaine.

Enfin, la mise en œuvre de telles mesures par la police judiciaire étant déjà très largement éprouvée par les magistrats et les procédures d'urgence nécessaires y ayant été développées pour que l'équilibre des droits et des objectifs poursuivis puisse être préservé par l'intervention d'une juridiction indépendante, il apparaît définitivement que le législateur ne pouvait se prévaloir d'aucun motif pour permettre les atteintes aux droits et libertés fondamentaux qu'il autorise sans les limiter par la seule garantie que le droit constitutionnel juge satisfaisante compte tenu de leur importance : l'autorisation de l'autorité judiciaire.

En conclusion,

La disproportion qui découle de l'absence de contrôle juridictionnel préalable des mesures de surveillance affectant l'ensemble des mesures autorisées aux articles 2 et 3 de la présente loi, celle-ci s'en trouve dans son ensemble contraire à la Constitution et doit dès lors être censurée.

10.3. Les imprécisions affectant le contrôle des autorisations

Les imprécisions affectant le contrôle des autorisations portent tant sur les personnes surveillées que sur les finalités en vue desquelles les mesures de surveillance sont mises en œuvre.

10.3.1. Imprécision sur les personnes surveillées

L'article L. 821-2 du CSI créé par la présente loi dispose que les demandes de mise en œuvre de techniques de renseignement par les services doivent préciser :

« 1° La ou les techniques à mettre en œuvre ;

« 2° Le service pour lequel elle est présentée ;

« 3° La ou les finalités poursuivies ;

« 4° Le ou les motifs des mesures ;

« 5° La durée de validité de l'autorisation ;

« 6° La ou les personnes, le ou les lieux ou véhicules concernés. »

L'article précise que, « pour l'application du 6°, les personnes dont l'identité n'est pas connue peuvent être désignées par leurs identifiants ou leur qualité et les lieux ou véhicules peuvent être désignés par référence aux personnes faisant l'objet de la demande ».

C'est au regard de cette demande que la CNCTR va contrôler — au moment de rendre son avis préalable ou plus tard — que les renseignements collectés sont proportionnés et utiles à la poursuite de l'objectif invoqué par les services.

En effet, l'article L. 801-1 du CSI créé par la présente loi dispose que la CNCTR « s'assure, dans les conditions prévues au présent livre, du respect [des] principes » prévus à cet article, et notamment celui exigeant que les mises en œuvre de techniques « sont justifiées par les menaces, les risques et les enjeux liés aux intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 » et que « les atteintes qu'elles portent au respect de la vie privée sont proportionnées aux motifs invoqués ».

Que la CNCTR réalise un contrôle de proportionnalité des techniques qu'elle surveille semble être la première des garanties que le législateur pouvait prévoir pour assurer le respect des droits et libertés mis en cause.

Néanmoins, tel contrôle apparaît comme illusoire dès lors qu'il porte, comme la présente loi le permet, sur un nombre indéfini de personnes. En effet, aucun contrôle de proportionnalité effectif ne peut porter sur plus d'une seule personne pour considérer concrètement la menace, le risque et les enjeux précis que sa surveillance représente pour les intérêts de la Nation.

Le défaut d'effectivité de ce contrôle est aggravé de ce que la présente loi prévoit qu'il peut porter sur des personnes non identifiées mais seulement définies par leur « qualité ». Or en raison de l'imprécision de cette notion la CNCTR pourra se retrouver à contrôler des techniques portant sur un très grand nombre de personnes et à ne pouvoir examiner la proportionnalité des atteintes ainsi portées aux droits de chacune d'elles que sur des critères particulièrement évasifs. Ces décisions juridiques emportant des effets considérables pour les droits et libertés des personnes en question seront donc prises sans aucune prise en compte des situations individuelles.

En conclusion,

En ce qu'elle prive la CNCTR de réaliser tout contrôle de proportionnalité effectif quant à la mise en œuvre des techniques qu'elle permet, la formule « La ou les personnes » du 6° de l'article L. 812-2 du CSI doit être censurée et réduite à « La personne », le législateur ayant échoué en l'employant à prévoir les garanties au respect de droits et libertés fondamentales que l'article 34 de la Constitution lui impose de prendre.

10.3.2. Imprécision sur les finalités poursuivies

Premièrement, l'ensemble des techniques de renseignement prévues au titre V du livre VIII du CSI, tel que créé par la présente loi, ne peut être mise en œuvre que « dans les

conditions prévues au chapitre Ier du titre II du présent livre », tel que le prévoit chacun des articles autorisant chacune d'elles.

Or, aucune des dispositions de ce chapitre Ier ne prévoit que leur mise en œuvre ne peut être autorisée que dans le seul but de poursuivre l'un des intérêts fondamentaux de la Nation visés à l'article L. 811-3 créé par la présente loi. En effet, le 3° de l'article L. 821-2 prévoit seulement que les demandes de mise en œuvre doivent préciser « la ou les finalités poursuivies », sans exiger que cette ou ces finalités soient de celles énumérées à l'article L. 811-3. Cette disposition ne peut être conforme à la Constitution que si elle est interprétée comme signifiant « la ou les finalités visées à l'article L. 811-3 du présent code poursuivies », auquel cas seulement elle permettrait de limiter effectivement les atteintes permises.

De même, cette interprétation ne peut produire tel effet que si le 4° du même article, prévoyant que les demandes précisent « le ou les motifs des mesures », est interprété comme signifiant « le ou les motifs, conformes à la ou aux finalités poursuivies par les mesures ».

Secondement, de telles modifications permettraient aussi de combler l'autre grave imprécision affectant les finalités poursuivies. En effet, l'article L. 822-3 du chapitre II du titre II du CSI prévoit que « les renseignements ne peuvent être collectés, transcrits ou extraits pour d'autres finalités que celles mentionnées à l'article L. 811-3 » et que « les transcriptions ou les extractions doivent être détruites dès que leur conservation n'est plus indispensable à la poursuite de ces finalités ».

De même, l'article L. 801-1 du CSI prévoit que les techniques de renseignement « sont justifiées par les menaces, les risques et les enjeux liés aux intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 ». Or, aucune de ces dispositions n'exige que les mises en œuvre des techniques autorisées ne puissent poursuivre aucune autre finalité que celle ou celles précisées dans leur demande d'autorisation et au regard desquelles la CNCTR réalise son contrôle de proportionnalité.

Ainsi, au regard de ces dispositions, les services de renseignement pourront recourir à une technique pour poursuivre n'importe laquelle des finalités prévues à l'article L. 811-3 dès l'instant où la mise en œuvre de cette technique aura été autorisée pour poursuivre une seule de ces finalités.

Dès lors, le contrôle de proportionnalité confié à la CNCTR se révèle illusoire, le législateur ayant échoué à limiter l'action des services à des finalités et des objectifs limités et précis au regard desquels la CNCTR peut effectivement réaliser son contrôle.

En conclusion,

La présente loi est contraire à la Constitution, notamment à son article 34, en ce qu'elle n'apporte pas les garanties aux droits et libertés fondamentaux auxquels elle autorise l'atteinte.

Néanmoins, l'imprécision sur les finalités poursuivies pourrait être corrigée par une réserve précisant que la première phrase du premier alinéa de l'article L. 822-3 doit être interprétée comme signifiant « les renseignements ne peuvent être collectés, transcrits ou extraits pour d'autres finalités que celles pour lesquelles leur traitement a été autorisé ».

10.4. L'insuffisance des garanties apportées aux professions dont le secret est protégé

Dans son rapport rendu pour avis au nom de la commission des affaires étrangères, de la défense et des forces armées du Sénat, M. Jean-Pierre Raffarin prétend que « *les dispositions adoptées pour protéger de façon légitime certaines professions ou fonctions (parlementaires, magistrats, avocats, journalistes) ont pris parfois un caractère d'interdiction absolue d'agir* » [12].

Cette description abusive fait l'impasse sur les lacunes dont souffrent les maigres garanties apportées en cours d'examen parlementaire au secret professionnel des professions protégées, et qui entachent le texte d'incompétence négative.

En droit,

Droit constitutionnel

Le Conseil constitutionnel attache une importance particulière au secret professionnel qui bénéficie d'une protection au titre du droit au respect de la vie privée. Ainsi, là où le Conseil a jugé conformes à la Constitution les dispositions du règlement concernant l'organisation et au fonctionnement de l'Assemblée nationale relatives aux pouvoirs de convocation et d'audition des commissions permanentes, c'est seulement après avoir souligné que :

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

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

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

Enfin, si le Conseil constitutionnel peut admettre que, dans certaines hypothèses, des personnes soient déliées de leur secret professionnel, c'est à la condition que le législateur l'ait dûment « prévu » et ce, aux termes d'une stricte « conciliation entre, d'une part, l'exercice des libertés constitutionnellement garanties, au nombre desquelles figure le droit

12. Jean-Pierre Raffarin, 2015. *Avis n° 445 (2014-2015) fait au nom de la commission des affaires étrangères, de la défense et des forces armées sur le projet de loi relatif au renseignement*, Sénat. Disponible à l'adresse : `http://www.senat.fr/rap/a14-445/a14-445.html`.

au respect de la vie privée et, d'autre part, les exigences de solidarité découlant des dixième et onzième alinéas du Préambule de 1946 » (Cons. constit. n° 2007-553 DC du 3 mars 2007, cons. 4 à 6).

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

Le secret des correspondances de certaines professions est toutefois particulièrement protégé par le code de procédure pénale. Il s'agit notamment des magistrats, avocats, parlementaires et journalistes (articles 226-13 et 226-14 du Code pénal), la préservation de leur indépendance étant considérée comme indispensable au bon fonctionnement de la démocratie.

La protection spéciale de ces professions ne découle pas seulement de l'article 2 de la déclaration de 1789, mais de sa lecture combinée avec l'article 16 et l'article 11, qui protègent les droits de la défense et le droit à procès équitable d'une part, et la liberté de communication d'autre part.

Droit européen

Pour sa part, la CEDH a condamné une mise sur écoute des lignes téléphoniques d'un cabinet d'avocats sur instruction du procureur général de la Confédération suisse, pour violation de l'article 8 de la convention, en l'absence de règles claires et détaillées du recours à ce dispositif, car ces écoutes étaient sans lien avec la procédure pénale en question. Si seules les activités relevant spécifiquement du mandat d'avocat sont couvertes par le secret professionnel, la loi doit cependant expliciter « *à quelles conditions et par qui relève spécifiquement du mandat d'avocat et ce qui a trait à une activité qui n'est pas celle de conseil* » (CEDH, *Kopp c. Suisse*, 25 mars 1998, n° 23224/94). Dans cet arrêt, la Cour critique également l'absence de contrôle par un magistrat indépendant sur les mesures de surveillance des communications de ce cabinet d'avocats (§ 74).

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

> *« En vertu de l'article 8, la correspondance entre un avocat et son client, quelle qu'en soit la finalité (...), jouit d'un statut privilégié quant à sa confidentialité (...). Elle a en outre indiqué qu'elle « accorde un poids singulier au risque d'atteinte au secret professionnel des avocats car il peut avoir des répercussions sur la bonne administration de la justice » (...) et est la base de la relation de confiance entre l'avocat et son client ».*
>
> (CEDH, *Michaud c. France*, 6 décembre 2012, n° 12323/11, §117)

Les journalistes ont un droit et un devoir de protéger l'anonymat de leurs sources lorsque leur éventuelle identification risque de nuire à leur liberté de parole, garanti par l'article 10 de la CESDH :

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

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

Eu égard à l'importance que revêt la protection des sources journalistiques pour la liberté de la presse dans une société démocratique et à l'effet négatif sur l'exercice de cette liberté que risque de produire une ordonnance de divulgation, pareille mesure ne saurait se concilier avec l'article 10 (art. 10) de la Convention que si elle se justifie par un impératif prépondérant d'intérêt public ».

(CEDH, *Goodwin c. Royaume-Uni*, 27 mars 1996, n° 17488/90, § 39)

La Cour de Strasbourg a également eu l'occasion de sougliner l'importance d'un contrôle distinct de l'exécutif sur les mesures portant atteinte à la confidentialité des sources :

« Au premier rang des garanties exigées doit figurer la possibilité de faire contrôler la mesure par un juge ou tout autre organe décisionnel indépendant et impartial. Le principe selon lequel, dans les affaires concernant la protection des sources des journalistes, « le tribunal doit pouvoir contempler le tableau complet de la situation » a été souligné dans l'une des toutes premières affaires de cette nature examinées par les organes de la Convention (...). ***Le contrôle requis doit être mené par un organe, distinct de l'exécutif*** *et des autres parties intéressées, investi du pouvoir de dire, avant la remise des éléments réclamés, s'il existe un impératif d'intérêt public l'emportant sur le principe de protection des sources des journalistes et, dans le cas contraire, d'empêcher tout accès non indispensable aux informations susceptibles de conduire à la divulgation de l'identité des sources ».*

(CEDH, *Sanoma Uitgevers B.V. c. Pays-Bas*, 14 septembre 2010, n° 38224/03, § 90)

Droit de l'Union européenne

Enfin, parmi les griefs retenus par la CJUE dans son arrêt *Digital Rights*[13] pour invalider la directive 2006/24/CE, la Cour de Luxembourg souligne que la conservation des données de connexion « s'applique donc **même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves**. En outre, elle ne prévoit aucune exception, de sorte qu'**elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel** » (§58). Cet arrêt met en lumière la nécessité d'apporter des garanties spéciales au secret des professions protégées.

10.4.1. Une protection insuffisante des avocats, magistrats et journalistes

En l'espèce,

La présente loi crée un article L. 821-7 au CSI, disposant que :

« Un parlementaire, un magistrat, un avocat ou un journaliste ne peut être l'objet d'une demande de mise en œuvre, sur le territoire national, d'une technique de recueil de

13. Voir développements *supra*, section 5.2.4 page 42.

renseignements mentionnée au titre V du présent livre à raison de l'exercice de son mandat ou de sa profession. Lorsqu'une telle demande concerne l'une de ces personnes ou ses véhicules, ses bureaux ou ses domiciles, l'avis de la Commission nationale de contrôle des techniques de renseignement est examiné en formation plénière. L'article L. 821-5 n'est pas applicable. L'article L. 821-6 n'est pas applicable, sauf s'il existe des raisons sérieuses de croire que la personne visée agit aux ordres d'une puissance étrangère, ou dans le cadre d'un groupe terroriste ou d'une organisation criminelle. »

En conclusion,

Compte tenu des lacunes déjà relevées s'agissant du contrôle préalable opéré par la CNCTR (voir *supra* 10 page 85), la présente loi échoue à apporter des garanties suffisantes à ces professions et viole la Constitution et le droit européen.

Par ailleurs, bien que les professions de parlementaire, de magistrat, d'avocat ou de journaliste échappent à la procédure d'urgence absolue prévue par le Gouvernement, qui prévoit que l'autorisation est donnée sans avis préalable de la CNCTR (article L. 821-5), elles peuvent toutefois faire l'objet d'une procédure d'urgence opérationnelle (sans autorisation préalable du Premier ministre) introduite par l'Assemblée nationale (article L. 821-6) [14].

Enfin, ces dispositions dérogatoires ne concernent que la surveillance des professionnels en cause, et non celle de leurs correspondants, n'assurant ainsi la protection d'aucun secret lorsqu'une mesure de surveillance vise ces derniers.

Ainsi, en échouant à apporter des garanties suffisantes au secret des correspondances des avocats, magistrats et journalistes, le législateur a violé les articles 2, 11, 16 de la Déclaration de 1789 et 34 de la Constitution.

10.4.2. Le champ des professions protégées est trop limité

Bien que le secret des correspondances des avocats et des journalistes revête une importance particulière, il existe d'autres professions dont le secret est protégé et qui justifient des garanties renforcées. Le législateur n'en a malheureusement pas tenu compte.

En l'espèce,

À cet égard, il est à noter que le livre VIII du CSI prend en compte une liste de professions plus restrictive que celle du code de procédure pénale, limitant donc sans aucune justification la portée de sa protection.

Ainsi, les huissiers, notaires ou professionnels de santé ne sont pas mentionnés dans l'exception aux procédures de renseignement, établie à l'article L. 821-7. Ces mêmes professions font cependant l'objet d'une protection particulière dans le code de procédure pénale. Le secret médical est ainsi reconnu par le code pénal (article 226-13) qui dispose que les professionnels de santé sont contraints de taire les informations personnelles concernant les patients qu'ils ont recueillies au cours de leur activité. Devant l'étendue des catégories de professionnels de santé liés par le secret médical, l'article L. 821-7 du CSI apparaît comme trop restrictif et porte une atteinte injustifiée à l'exercice légitime de leurs fonctions.

De même que les professeurs d'université et maîtres de conférence sont exclus de ce

14. Sur les procédures d'urgence, voir section 10.2.2.3 page 94.

régime spécial, alors même que la Constitution garantit « l'indépendance des professeurs d'université » et, plus généralement, des enseignants-chercheurs, en tant que principe fondamental reconnu par les lois de la République (Cons. const., décision n° 83-165 DC, 20 janvier 1984, cons. 17 à 28).

En conclusion,

Le champ des professions disposant de garanties spéciales est trop restrictif pour assurer une conciliation équilibrée entre les intérêts d'ordre public et les droits en présence.

11. Contrôle a posteriori

11.1. L'absence de transparence sur les abus et situations d'illégalité viole le droit à l'information

Dans cette section sont examinées successivement la procédure créée pour les lanceurs d'alerte au bénéfice des agents des services de renseignement (article L. 861-3), puis la disposition réprimant la révélation des mesures de surveillance (articles L. 833-4), celle sur le rapport d'activité de la CNCTR (L. 881-1), et celle sur les décisions du Conseil d'État dans le cadre des recours contentieux (article L. 773-7 du code de justice administrative) qui, de concert, organisent l'opacité sur les abus et situations d'illégalité constatées dans les pratiques des services de renseignement.

11.1.1. La procédure de signalement pour les lanceurs d'alerte est trop restrictive

Un amendement à l'Assemblée nationale a créé un statut spécial pour les lanceurs d'alerte à l'article L. 861-3. Ce dernier dispose notamment :

> *« **Art. L. 861-3–I**. – Tout agent d'un service mentionné à l'article L. 811-2 ou d'un service désigné par le décret en Conseil d'État prévu à l'article L. 811-4 qui a connaissance, dans l'exercice de ses fonctions, de faits susceptibles de constituer une violation manifeste du présent livre peut porter ces faits à la connaissance de la seule Commission nationale de contrôle des techniques de renseignement, qui peut alors saisir le Conseil d'État dans les conditions prévues à l'article L. 833-8 et en informer le Premier ministre ».*

Cet ajout constitue une modalité supplémentaire du contrôle *a posteriori* des mesures secrètes de surveillance. La disposition est cependant trop limitée dans sa portée pour protéger le droit à l'information, garantie essentielle pour prévenir de l'arbitraire qui résulterait d'abus dans les pratiques de surveillance secrète. Pour cette raison, cet amendement viole en fait les articles 2 et 11 de la Déclaration de 1789.

En droit,

L'absence de jurisprudence spécifique du Conseil constitutionnel sur les lanceurs d'alerte invite à se tourner vers la jurisprudence de la CEDH et les standards internationaux en vigueur.

11.1.1.1. Droit européen

En ce qui concerne la protection des lanceurs d'alerte, la Grande chambre de la Cour de Strasbourg a établi les principes suivants dans son arrêt fondateur *Guja c. Moldavie*, en date du 12 février 2008 :

> *« (...) [L']article 10 s'applique également à la sphère professionnelle et (...) les fonctionnaires (...) jouissent du droit à la liberté d'expression (...). Cela étant, elle n'oublie pas que les salariés ont un devoir de loyauté, de réserve et de discrétion envers leur employeur. Cela vaut en particulier pour les fonctionnaires, dès lors que la nature même de la fonction publique exige de ses membres une obligation de loyauté et de réserve (...)*
>
> *« La mission des fonctionnaires dans une société démocratique étant d'aider le gouvernement à s'acquitter de ses fonctions et le public étant en droit d'attendre que les fonctionnaires apportent cette aide et n'opposent pas d'obstacles au gouvernement démocratiquement élu, l'obligation de loyauté et de réserve revêt une importance particulière les concernant (...). De plus, eu égard à la nature même de leur position, les fonctionnaires ont souvent accès à des renseignements dont le gouvernement, pour diverses raisons légitimes, peut avoir un intérêt à protéger la confidentialité ou le caractère secret. Dès lors, ils sont généralement tenus à une obligation de discrétion très stricte.*
>
> *« (...) En ce qui concerne les agents de la fonction publique, qu'ils soient contractuels ou statutaires, la Cour observe qu'ils peuvent être amenés, dans l'exercice de leur mission, à prendre connaissance d'informations internes, éventuellement de nature secrète, que les citoyens ont un grand intérêt à voir divulguer ou publier. Elle estime dans ces conditions que la dénonciation par de tels agents de conduites ou d'actes illicites constatés sur leur lieu de travail doit être protégée dans certaines circonstances. Pareille protection peut s'imposer lorsque l'agent concerné est seul à savoir – ou fait partie d'un petit groupe dont les membres sont seuls à savoir – ce qui se passe sur son lieu de travail et est donc le mieux placé pour agir dans l'intérêt général en avertissant son employeur ou l'opinion publique. (...)*
>
> *« Eu égard à l'obligation de discrétion susmentionnée, il importe que la personne concernée procède à la divulgation d'abord auprès de son supérieur ou d'une autre autorité ou instance compétente. La divulgation au public ne doit être envisagée qu'en dernier ressort, en cas d'impossibilité manifeste d'agir autrement (...). Dès lors, pour juger du caractère proportionné ou non de la restriction imposée à la liberté d'expression du requérant en l'espèce, la Cour doit examiner si l'intéressé disposait d'autres moyens effectifs de faire porter remède à la situation qu'il jugeait critiquable.*
>
> *« Pour apprécier la proportionnalité d'une atteinte portée à la liberté d'expression d'un fonctionnaire en pareil cas, la Cour doit également tenir compte d'un certain nombre d'autres facteurs. Premièrement, il lui faut accorder une attention particulière à l'intérêt public que présentait l'information divulguée. La Cour rappelle que l'article 10 § 2 de la Convention ne laisse guère de place pour des restrictions à la liberté d'expression dans le domaine des questions d'intérêt général (...). Dans un système démocratique, les actions ou omissions du gouvernement doivent se trouver placées sous le contrôle attentif non seulement des pouvoirs législatif et judiciaire, mais aussi des médias et de l'opinion publique. L'intérêt de l'opinion publique pour une certaine information peut parfois être si grand qu'il peut l'emporter même sur une obligation de confidentialité imposée par la loi (...) »*
>
> (CEDH, 12 février 2008, *Guja c. Moldavie*, n° 14277/04, §§70-74).

Dans une autre affaire jugée en janvier 2013, la CEDH a étendu cette jurisprudence aux mesures de surveillance secrète, en invalidant la condamnation d'un agent des services

secrets roumains. Ce dernier avait révélé à l'occasion d'une conférence de presse des informations classifiées « ultra-secret » (enregistrement audio notamment) démontrant la mise sur écoute arbitraire de journalistes, de personnalités politiques et d'hommes d'affaires. Dans sa décision, les juges rappellent qu'« il n'appartient pas à la Cour de se substituer aux États parties à la Convention dans la définition de leurs intérêts nationaux, domaine qui relève traditionnellement du noyau dur de la souveraineté étatique ». Ils soulignent néanmoins la nécessité de permettre que les « abus » liés aux activités de surveillance secrète puissent être divulgués au public :

> *« (...) la Cour estime que les informations divulguées par le requérant avaient un rapport avec des abus commis par des fonctionnaires de haut rang et avec les fondements démocratiques de l'État. Il ne fait désormais aucun doute qu'il s'agit là de questions très importantes relevant du débat politique dans une société démocratique,* ***dont l'opinion publique a un intérêt légitime à être informée*** *».*
> (CEDH, 8 janvier 2013, *Bucur et Toma c. Roumanie*, n° 40238/02, §103).

11.1.1.2. Principes mondiaux sur la sécurité nationale et le droit à l'information

En 2013, sous l'égide de l'Open Society Justice Initiative, une équipe d'experts internationaux a travaillé à l'élaboration de principes détaillés permettant de trouver un juste équilibre entre le recours légitime au secret d'État et la garantie du droit à l'information [1]. Dix-sept organismes, dont de nombreuses ONG et des centres de recherche en droit, et plus de 500 experts issus des quatre continents ont participé à leur rédaction. Publiés au printemps 2013, ils ont à ce titre vocation à faire consensus. La recommandation 2014(7) du Comité des ministres du Conseil de l'Europe sur la protection des lanceurs d'alerte y fait d'ailleurs référence [2].

Le constat sur lequel se fondent ces principes est celui d'un droit gravement lacunaire : « *le droit international fait preuve d'une considérable déférence à l'égard des décisions des gouvernements nationaux au sujet des mesures nécessaires à la protection de la sécurité nationale* ». Or, la « *sur-invocation de risques pour la sécurité nationale peut sérieusement remettre en cause les principaux garde-fous institutionnels contre les abus : l'indépendance de la justice, l'État de droit, le contrôle du législateur, la liberté de la presse, un gouvernement transparent* ». Plusieurs principes regroupés dans la partie relative à la « divulgation d'intérêt public par le personnel public » [3] proposent de remédier à ces lacunes en apportant une protection pleine et entière aux lanceurs d'alerte. Le principe 37 rappelle ainsi la nécessité d'assurer une protection des lanceurs d'alerte pour la dénonciation d'un champ très large d'abus et autres « méfaits » dont ils seraient témoins et que « *la loi doit protéger des représailles les personnels publics qui divulguent des informations mettant des méfaits en évidence, que lesdites informations soient classifiées, confidentielles ou non* ». Une telle protection doit être assurée à la fois dans le

1. Principes mondiaux sur la sécurité nationale et le droit à l'information (principes de Tschwane), *Open Society Foundations*, 12 juin 2013. Disponible à l'adresse : `http://www.opensocietyfoundations.org/publications/global-principles-national-security-and-right-information-tshwane-principles/fr`.

2. Comité des ministres du Conseil de l'Europe, *Recommandation CM/Rec(2014)7 sur la protection des lanceurs d'alerte*, Strasbourg, p. 29. Disponible à l'adresse : `https://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec%282014%297F.pdf`.

3. *Idem*, p. 57.

cadre de procédures internes (principe 39) mais également dans le cadre de divulgations publiques, par exemple *via* la presse, notamment dans le cas où, suite à une alerte interne, la « *personne n'a pas reçu de résultats raisonnables et appropriés dans un délai raisonnable* » ou si :

> *« La personne a des motifs raisonnables de penser qu'il existe un risque significatif qu'une divulgation interne et/ou auprès d'un organisme indépendant de surveillance entraîne la destruction ou la dissimulation des preuves, des interférences avec des témoins ou des représailles à l'encontre de la personne ou d'un tiers ».*
> *(Principe 40).*

En l'espèce,

Avec l'ajout de cet article L. 861-3, le Parlement reprend les recommandations émises par le Conseil d'État dans son étude publiée en septembre 2014, qui proposait la création d'une telle procédure auprès de la CNIL pour le signalement d'abus dans les usages des données des services de renseignement.

En toute fin d'examen parlementaire, au moment du vote du texte de la Commission mixte paritaire au Sénat le 23 juin, le Gouvernement est parvenu à faire adopter un amendement supprimant l'alinéa 10 de cette disposition, lequel disposait :

> *« L'agent mentionné au précédent alinéa peut, dans le seul cadre de la relation ou du témoignage réalisé devant la commission, faire état d'éléments ou d'informations protégés au titre du secret de la défense nationale ou susceptibles de porter atteinte à la sécurité des personnels ou des missions des services mentionnés à l'alinéa précédent ».*

Dans son exposé des motifs, le gouvernement s'est justifié en expliquant que :

> « Cet amendement de précision garantit que la sécurité des personnels ne sera pas mise en danger de ce fait, ni le bon déroulement des missions légitimes entravé ».

Sauf qu'avec cette suppression, le Gouvernement a complètement remis en cause l'effectivité de cette procédure d'alerte en créant une grande insécurité juridique pour les lanceurs d'alerte potentiels, montrant par là-même sa formidable défiance à l'idée même d'un contrôle effectif de la CNCTR. Le gouvernement ne peut en effet sérieusement prétendre que l'action de la CNCTR risquerait — une fois alertée par un agent d'une illégalité et alors même que ses membres et son personnel sont habilités au secret (article L. 832-5) — de mettre en cause le secret de la défense nationale, de mettre en danger des personnels ou de nuire au bon déroulement de ces missions. Le but manifeste de cet amendement étant de priver d'effectivité l'ensemble de l'article L. 861-3, une réserve d'interprétation doit rappeler l'évidence, à savoir que l'agent est libre de livrer toute information nécessaire à la réalisation des missions de la CNCTR.

Ensuite, même dans le texte adopté en Commission mixte paritaire, le champ de cette disposition demeure trop étroit. L'article L. 861-3 se limite aux « faits susceptibles de constituer une violation manifeste du présent livre », à savoir le livre VIII du code de la sécurité intérieure relatif au renseignement. Ce alors que nombre d'abus dont la révélation serait d'intérêt public touchent davantage à des infractions qui ne relèvent pas du code de la sécurité intérieure. Certes, l'article 851-7 dispose que :

> *« Le présent chapitre est mis en œuvre dans le respect de l'article 226-15 du code pénal*[4] *».*

4. L'article 226-15 du code pénal dispose :

Pour autant, le chapitre en question (chapitre premier du titre V) ne traite que des « accès administratifs aux données de connexion », laissant ainsi de côté un grand nombre de techniques de renseignement ainsi que de nombreuses autres infractions sanctionnant des atteintes à la vie privée.

À rebours de ce que laisse penser la lecture du seul article L. 851-7, il est certes possible d'interpréter la loi de sorte que l'ensemble des infractions protectrices de la vie privée et du secret des correspondances incluses dans le code pénal soient indirectement couvertes par l'article L. 801-1, lequel dispose :

> *« Le respect de la vie privée, dans toutes ses composantes, notamment le secret des correspondances, la protection des données personnelles et l'inviolabilité du domicile, est garanti par la loi. L'autorité publique ne peut y porter atteinte que dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité ».*

Hélas, une telle interprétation n'est pas explicite.

Surtout, bien d'autres abus potentiels — liés par exemple à des cas de corruption active (article L. 433-1 du code pénal) au sein des services de renseignement — resteraient alors hors du champ de cette procédure d'alerte. **Il est donc nécessaire d'élargir le champ des infractions couvertes par l'article L. 861-3 en visant, outre le livre VIII du code de la sécurité intérieure, l'ensemble des crimes et délits**.

Toutefois, l'article L. 861-3 risquerait alors de paraître antagoniste des dispositions de l'article 40 du code de procédure pénale. Ce dernier prévoit notamment que :

> *« Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs ».*

Il importe de rappeler à cet égard que le respect de cette obligation qui incombe aux agents de la fonction publique est particulièrement délicat dans le cadre des activités de renseignement. En effet, un agent qui porte à la connaissance du procureur de tels crimes et délits s'exposera le plus souvent à des poursuites pour violation du secret de la défense nationale. Dès lors, en parallèle de l'élargissement de l'article L. 861-3 à tout crime ou délit, les lanceurs d'alerte doivent être immunisés contre l'application de l'article 40 du code de procédure pénale lorsqu'ils rapportent des faits à la seule CNCTR sans les porter à la connaissance du procureur. Le procureur devra alors être avisé par le Conseil d'État, lequel sera saisi sans délai par la CNCTR dès qu'elle constate ou est informée de la commission d'illégalités ou de faits susceptibles de constituer des infractions pénales (tel que défendu *infra*, section 11.2.2 page 113). Le Conseil d'État devra également être

---

> *« Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende.*
>
> *« Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions. »*

compétent pour déclassifier lui-même certains documents liés aux requêtes qu'il instruit, notamment en vue de les transmettre au procureur (voir *infra*, section 11.3.2 page 118).

Enfin, la notion de « violation manifeste » crée une insécurité juridique pour les lanceurs d'alerte qui ne peut que conduire à ce que se prolongent des atteintes injustifiables aux droits et libertés. À l'image de la notion du « manifestement illicite » dans la jurisprudence constitutionnelle relative à la LCEN [5], elle ne repose de manière assez paradoxale sur aucun critère juridique intelligible, et n'apporte aucun sens précis à la disposition, et sera donc vecteur d'arbitraire au cours de l'application de la norme par les pouvoirs exécutifs et juridictionnels. L'adjectif « manifeste » ne sert en fait qu'à permettre le maintien de l'opacité sur des situations illégales voire constitutives de crimes ou de délits mais qui ne seraient pas nécessairement perçues comme tels parce que ne constituant pas aux yeux de l'agent une violation *manifeste* du code de la sécurité intérieure.

En conclusion,

Pour respecter l'article 2 et l'article 11 de la déclaration de 1789, l'article L. 861-3-I doit faire l'objet de plusieurs réserves d'interprétation.

La première doit priver d'effet l'amendement gouvernemental supprimant l'alinéa 10 de l'ancien article 3 bis afin de ne pas priver de toute effectivité l'article L. 861-3, une réserve d'interprétation doit rappeler l'évidence, à savoir que l'agent est libre de livrer toute information nécessaire à la réalisation des missions de la CNCTR.

La deuxième doit préciser que cette disposition concerne, outre le livre VIII du code de la sécurité intérieure, le signalement de tout crime ou délit. Cette réserve d'interprétation devrait également souligner que l'article 40 alinéa 2 du code de procédure pénale n'est pas applicable aux fonctionnaires qui signalent à la CNCTR des faits susceptibles de constituer des infractions pénales.

Enfin, l'adjectif « manifeste » situé après « violation » doit être censuré en ce qu'il nuit à l'intelligibilité de la disposition et risque de contribuer à la rendre inopérante en créant une insécurité juridique pour les agents qui souhaiteraient faire un signalement auprès de la CNCTR.

11.1.2. Aucune publicité n'est permise sur les abus liés à la surveillance secrète

La loi interdit formellement les divulgations publiques, même lorsque celles-ci seraient conformes aux normes et standards internationaux en matière de liberté d'expression. L'article 13 élargit en effet l'incrimination prévue à l'article L. 881-1 du code de la sécurité intérieure (actuellement l'article L. 245-1 du même code) au fait de révéler non plus seulement l'exécution d'une décision ou une opération d'interception, mais désormais l'exécution de toute « *technique de recueil de renseignement* » ou la simple « *existence de la mise en œuvre de cette technique* ». Ainsi, le fait de révéler à la presse ou de divulguer publiquement par tout autre moyen l'existence d'abus ou même de crimes et délits dans les activités de surveillance, alors même qu'une telle divulgation serait d'intérêt public

5. La Quadrature du Net, *Projet de loi pour l'égalité entre les femmes et les hommes : Non à la censure privée du Net*, Lettre et proposition d'amendement aux sénateurs, 25 mars 2014. Disponible à l'adresse :`https://www.laquadrature.net/files/PJL%20Egalite%20FH%20-%20analyse%20art.%2017%20-%20LQDN.pdf`.

et que l'alerte interne à l'administration serait objectivement risquée ou inefficace, est constitutif d'une infraction pénale.

Il en ressort que le champ de cette incrimination dépasse très largement les seules informations et données administratives couvertes par le secret de la défense nationale. Sa portée très large est d'autant plus disproportionnée que, dans le même temps, la loi facilite le fait pour l'autorité administrative de détruire, de cacher ou de dissimuler des preuves, puisque le texte invite la CNCTR à « informer » l'autorité de tutelle des services, à savoir le Premier ministre, des signalements qu'elle reçoit. En outre, même dans les cas où l'alerte interne fonctionnerait et que la CNCTR se décidait à saisir le Conseil d'État, l'information du public resterait entravée par le secret de la défense nationale, le Premier ministre restant maître des procédures de déclassification (voir section 11.3.2 page 118).

L'entrave au droit à l'information auquel aboutit l'article L. 881-1 participe en fait de l'économie générale du texte, qui interdit toute réelle transparence, et ce non seulement concernant les situations d'illégalité constatées par la CNCTR et le Conseil d'État s'agissant des autorisations illégales qui seraient délivrées, mais aussi tout autre abus lié à la mise en œuvre des techniques de renseignement. En effet, l'article L. 833-9 relatif au rapport d'activité de la CNCTR n'autorise la transparence que sur :

- 1° le nombre de demandes dont elle a été saisie et d'avis qu'elle a rendus ;
- 2° le nombre de réclamations dont elle a été saisie ;
- 3° le nombre de recommandations qu'elle a adressées au Premier ministre et de suites favorables données à ces recommandations ;
- 4° le nombre d'observations qu'elle a adressées au Premier ministre et d'avis qu'elle a rendus sur demande ;
- 5° le nombre d'utilisations des procédures d'urgence définies aux articles L. 821-5 et L. 821-6 ; de recours dont elle a saisi le Conseil d'État et de recours pour lesquels elle a produit des observations devant lui.

Dans le même temps, aucune transparence n'est permise au niveau des décisions du Conseil d'État (voir section 11.3 page 114). L'article L. 773-7 du code de la justice administrative créé par la loi déférée ne prévoit en effet aucune publicité s'agissant de la jurisprudence de la formation spéciale du Conseil d'État. Le requérant et plus encore le public ne bénéficient d'aucune information précise au-delà du simple fait qu'une irrégularité a été constatée. Une absence de transparence qui contraste par exemple avec les règles applicables au Royaume-Uni, où elles s'avèrent encore manifestement insuffisantes [6]. Cette opacité contrevient également directement au principe 28(b) des principes de Tshwane, lequel dispose que :

> « (...) Les jugements de cour – qui exposent l'ensemble des ordres de la cour, les conclusions essentielles, les preuves et l'argumentaire légal – doivent être rendus publics ».

Au final, *aucune transparence n'est donc possible sur le nombre de situations d'illégalité et d'infractions mises à jour par les deux principales instances de contrôle des services de renseignement.* Il n'est permis aucune information du public sur les activités illégales du pouvoir exécutif en matière de surveillance secrète, la nature des faits constitutifs d'infractions pénales et la commission même de ces infractions restant couvertes par le secret.

6. Pour une illustration récente, voir : Owen Bowcott. GCHQ's surveillance of two human rights groups ruled illegal by tribunal, *The Guardian*, 22 juin 2015. Disponible à l'adresse : `http://www.theguardian.com/uk-news/2015/jun/22/gchq-surveillance-two-human-rights-groups-illegal-tribunal`.

En conclusion,

L'article L. 881-1 doit faire l'objet d'une réserve d'interprétation explicitant le fait qu'il s'applique uniquement dans les cas où la divulgation d'informations relatives aux activités de surveillance secrète, et notamment à l'existence ou à l'exécution d'une technique de renseignement, viole non seulement le secret de la défense nationale mais qu'une telle violation n'est par ailleurs pas justifiée par le caractère d'intérêt public des informations révélées (auquel cas une sanction proportionnée au préjudice occasionné pour l'État est légitime).

À l'article L. 833-9 du code de la sécurité intérieure relatif au rapport d'activité de la CNCTR, une réserve d'interprétation doit ainsi être faite pour imposer la mention dans ce rapport du nombre d'avis non conformes émis par cette dernière ainsi que du nombre de mesures liées aux techniques de renseignement reconnues comme illégales par le Conseil d'État, en précisant les personnes visées et les techniques employées.

Sous ces réserves seulement, ces dispositions sont conformes à la Constitution.

11.2. Le contrôle a posteriori de la CNCTR est inopérant

Le contrôle réalisé *a posteriori* par la CNCTR défini aux articles L. 833-1 et suivants doit permettre à la CNCTR de faire cesser, à un stade pré-contentieux, des atteintes illégales constatées, à défaut d'avoir pu les prévenir en amont. Or, l'effectivité de ce contrôle n'est pas assurée. [7].

11.2.1. Un contrôle trop restreint puisqu'il ne concerne pas les opérations non-autorisées

En effet, l'article L. 822-1 du code de la sécurité intérieure prévoit que « le Premier ministre organise la traçabilité de la mise en œuvre des techniques autorisées [...] et définit les modalités de la centralisation des renseignements collectés. » Au regard de quoi l'article L. 833-2, 2° du même code prévoit que « pour l'accomplissement de ses missions, la commission [...] 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, ainsi qu'aux dispositifs de traçabilité des renseignements collectés et aux locaux où sont centralisés ces renseignements en application de l'article L. 822-1 ».

Concrètement, le contrôle de la légalité des techniques exige pour la CNCTR de pouvoir vérifier que les services de renseignement n'ont collecté aucune information correspondant à d'autres objectifs que ceux invoqués pour en autoriser la collecte, concernant une autre personne que celle visée par cette autorisation ou dont le délai de conservation est expiré. **Ces vérifications, réalisées le cas échéant au cours de contrôles inopinés, exigent que la CNCTR ait accès non pas seulement aux registres**

7. Pour rappel, le contrôle *a posteriori* des mesures de surveillance internationale fait l'objet de développements à la section 9.3.3 page 75

relatifs aux informations collectées suite à autorisation mais à l'ensemble des informations et données collectées par les services de renseignement, avec ou sans autorisation.

Or, la CNCTR n'a concrètement accès qu'aux renseignements que le Premier ministre a préalablement centralisés dans les locaux mentionnés à l'article L. 833-2, 2° précité selon les « modalités » qu'il « définit ». Dès lors, la CNCTR ne peut exercer aucun contrôle sur les renseignements que le Premier ministre exclurait de ces locaux, sans qu'elle ne puisse l'en empêcher d'aucune façon — n'ayant pas même conscience de l'existence de ces renseignements. De ce point de vue, l'amendement de la Commission mixte paritaire au 4° de l'article 833-2, qui prévoit que la CNCTR « *peut solliciter du Premier ministre tous les éléments nécessaires à l'accomplissement de ses missions,* ***y compris lorsque la technique de recueil de renseignement mise en œuvre n'a fait l'objet ni d'une demande, ni d'une autorisation*** *ou ne répond pas aux conditions de traçabilité*, constitue un faible progrès dès lors que cette communication est une fois encore soumise à la discrétion du Premier ministre.

En conclusion,

Pour que le contrôle *a posteriori* de la CNCTR, notamment sous la forme de visites inopinées dans les locaux de l'administration, soit pleinement effectif, la collecte des renseignements aurait dû être placée sous son contrôle et sa seule autorité — tel que les investigations judiciaires sont placées sous le contrôle et l'autorité du juge — ce qui, en l'espèce, aurait eu pour conséquence technique de confier directement la centralisation de l'ensemble des informations collectées par tout service à la CNCTR, et non au Premier ministre que cette dernière est censée contrôler. Le Gouvernement et le Parlement en ont toutefois décidé autrement, bien que des amendements aient été adoptés en vue d'assurer une plus grande centralisation des renseignements collectés.

Subsidiairement,

A minima, l'article L. 833-2, 2°, doit faire l'objet d'une réserve d'interprétation pour préciser que l'accès permanent, complet et direct de la CNCTR aux relevés, registres, renseignements collectés, transcriptions et extractions ainsi qu'aux dispositifs de traçabilité des renseignements collectés et aux locaux où sont centralisés ces renseignements vaut « *y compris lorsque la technique de recueil de renseignement mise en œuvre n'a fait l'objet ni d'une demande, ni d'une autorisation ou ne répond pas aux conditions de traçabilité* ».

11.2.2. Une saisine du Conseil d'État optionnelle lorsque des illégalités sont constatées

Lorsqu'au cours de ses investigations, la CNCTR constatera qu'une technique a été mise en œuvre en violation de la présente loi voire qu'elle prendra connaissance de faits susceptibles de constituer des infractions pénales, elle ne pourra qu'adopter des recommandations et, seulement si l'administration échoue à suivre ces recommandations (article L. 833-6) ou si un lanceur d'alerte lui signale de tels abus (voir section 11.1.1), elle *pourra* saisir le Conseil d'État (article L. 833-8).

Combiné au caractère non contraignant des recommandations de la CNCTR au Premier ministre, le caractère facultatif de cette saisine risque de laisser se perpétuer des illégalités profondément attentatoires aux droits et libertés des citoyens au cas où, pour

une raison ou une autre, la CNCTR choisirait de ne pas saisir le Conseil d'État, ou qu'elle attendrait trop longtemps avant d'estimer que le Premier ministre échoue à donner suite à ses recommandations et qu'une saisine juridictionnelle s'impose.

Par ailleurs, la saisine du Conseil d'État peut prendre la forme des référés (article 311-4-1 alinéa 2 du code de justice administrative), mais rien ne l'impose. Le risque existe donc que, même lorsqu'un contrôle juridictionnel est sollicité par la CNCTR et à défaut de mesures **suspensives**, celui-ci intervienne plusieurs semaines voire plusieurs mois après que les mesures ont commencé à porter atteinte aux droits et libertés, voire après que la CNCTR a constaté des faits susceptibles de constituer une situation d'illégalité.

En conclusion,

L'article L. 833-3 alinéa 2 et l'article L. 833-8 doivent être interprétés comme signifiant que, lorsque le Premier ministre informe « sans délai » la CNCTR qu'il n'a pas donné suite à ses recommandations en vertu de l'article L. 833-7, I, ou que la Commission estime ces suites insuffisantes, cette dernière *doit saisir sans délai le Conseil d'État afin que ce dernier statue en la forme des référés.*

L'article L. 861-3-I doit être interprété comme signifiant qu'en cas de signalement de faits susceptibles de constituer une illégalité par des lanceurs d'alerte, la CNCTR *doit saisir sans délai le Conseil d'État afin que ce dernier statue en la forme des référés.*

Sous ces réserves seulement, les dispositions en cause ne sont pas contraires à la Constitution.

11.3. Le recours contentieux ne respecte pas les droits de la défense

La présente loi définit les conditions dans lesquelles un contrôle juridictionnel *a posteriori* des mesures de surveillance peut être opéré par le Conseil d'État. Avec les articles L. 773-1 CJA et suivants, le secret-défense entre pour la première fois dans le système juridictionnel français[8].

En omettant d'assortir l'introduction du secret-défense dans le contentieux français des garanties nécessaires au maintien d'un équilibre, ne serait-ce que relatif entre les parties, cette procédure s'inscrit en violation des articles 6 et 16 de la Déclaration de 1789.

11.3.1. Une rupture absolue de l'égalité des armes

En droit,

8. « *La notion de "preuve secrète" n'existe pas en droit français car un document ou une information confidentiels ne peuvent pas être communiqués aux juges. Dès lors ils ne peuvent être utilisés comme preuve* ». Didier Bigo et al., National Security and Secret Evidence in Legislation and Before the Courts : Exploring the Challenges. Étude pour la commission Libertés civiles, justice et affaires intérieures du Parlement européen, Bruxelles. Disponible à l'adresse : `http://www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU%282014%29509991_EN.pdf`, p. 29 et p. 96 (traduction libre de : *The notion of "secret evidence" does not exist in French law, because a confidential document or information may not be communicated to the judges. Therefore, it cannot be used as evidence.*)

Dans sa décision n° 2010-15/23 QPC du 23 juillet 2010, Région Languedoc-Roussillon et autres (article 575 du code de procédure pénale), le Conseil constitutionnel énonçait, au regard des articles 6 et 16 de la Déclaration de 1789, que :

> *« si le législateur peut prévoir des règles de procédure différentes selon les faits, les situations et les personnes auxquelles elles s'appliquent, c'est à la condition que ces différences ne procèdent pas de distinctions injustifiées et que soient assurées aux justiciables des garanties égales, notamment quant au respect du principe des droits de la défense, qui implique en particulier l'existence d'une procédure juste et équitable garantissant l'équilibre des droits des parties »*
>
> (considérant 4)

Le Conseil estime par ailleurs dans une récente décision que :

> *« Tant le principe de la séparation des pouvoirs que l'existence d'autres exigences constitutionnelles imposent 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)

Par ailleurs, dans la jurisprudence de la CEDH sur les mesures de surveillance secrète, le droit au procès équitable implique que toutes les difficultés causées à la défense par une limitation de ses droits soient suffisamment compensées par la procédure suivie devant les autorités judiciaires [9].

En l'espèce,

Les articles L. 773-6 et L. 773-7 du code de la justice administrative tels qu'institués par la loi déférée sont porteurs de cette rupture abusive de l'équilibre des parties.

L'article L. 773-6 du code de la justice administrative dispose 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, soit parce que la personne concernée n'a fait l'objet d'aucune de ces mesures de surveillance, soit parce que ces mesures ont été mises en œuvre régulièrement, 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. »*

L'article L. 773-7 du code de la justice administrative dispose que :

> *« Lorsque la formation de jugement constate qu'une technique de recueil de renseignement est ou a été mise en œuvre illégalement ou qu'une donnée ou un renseignement a été conservé illégalement, elle peut annuler l'autorisation et ordonner la destruction des renseignements irrégulièrement collectés.*
>
> *« Sans faire état d'aucun élément protégé par le secret de la défense nationale, elle informe le requérant ou la juridiction de renvoi qu'une illégalité a été commise. Saisie de conclusions en ce sens lors d'une requête concernant la mise en œuvre d'une technique de renseignement ou ultérieurement, elle peut condamner l'État à indemniser le préjudice subi. »*

9. Voir par exemple *Doorson c. Pays-Bas*, 26 mars 1996, n° 20524/92, § 70 ; *Jasper c. Royaume-Uni* [GC], 16 février 2000 ; n° 27052/95, §§ 51-53, ; et *A. et autres c. Royaume-Uni* [GC], 19 février 2009, n° 3455/05, § 205).

La procédure ici en cause devant le Conseil d'État viole indûment le principe d'une procédure équitable garantissant l'équilibre des droits des parties. Alors que le requérant ne sait pas quelles mesures ont été prises contre lui, l'administration, elle, le sait. Alors que l'administration a accès à l'ensemble des pièces du dossier, le requérant, lui, n'a accès à rien. Alors que l'administration aura accès à l'ensemble du corpus jurisprudentiel pertinent par recoupement des mesures qu'elle aura mises en œuvre et des décisions qui auront été adoptées par le Conseil d'État, le requérant, une fois de plus, n'aura accès à rien. Il sera seulement informé qu'il a été victime d'une illégalité, sans qu'aucune information claire et précise sur la nature de celle-ci ne puisse lui être communiquée, puisque ces éléments seront couverts par le secret.

Au surplus, le requérant ne pourra pas accéder aux arguments développés par l'administration lors des audiences à huis clos (article L. 733-4). En somme, le requérant et son éventuel représentant sont totalement aveuglés et démunis de tout moyen. Et personne d'autre que l'administration et le juge spécialisé ne connaîtra le droit applicable aux mesures de surveillance. Les termes de l'article L. 773-3 du code de la justice administrative selon lesquels « [l]es exigences de la contradiction mentionnées à l'article L. 5 sont adaptées à celles du secret de la défense nationale » sont donc destinés à rester lettre morte puisque ces exigences ne sont aucunement adaptées mais anéanties.

11.3.1.1. Aucune disposition ne permet de compenser efficacement la rupture de l'égalité des armes

Le législateur était pourtant en mesure de remplir *a minima* son office en adoptant des mesures destinées à compenser cette rupture de l'égalité des armes. En témoignent des législations étrangères qui, bien que très critiquables sur de nombreux autres points, ont au moins mis en place un système dédié à la représentation des justiciables dans les matières comme le renseignement où le secret-défense peut prévaloir. Il en va ainsi des procédures juridictionnelles de supervision des activités de renseignement instituées au Royaume-Uni par le *Justice and Security Act* de 2013. Dans le cadre de la "*closed material procedure*" instituée par l'article 6 du Justice and Security Act, les justiciables sont représentés par des "*special advocates*" institués par l'article 9 de la même loi.

Le rôle et les pouvoirs des avocats spéciaux sont résumés comme suit par les auteurs d'une étude commanditée par le Parlement européen : « les avocats spéciaux sont des juristes habilités au secret qui sont autorisés à participer à des procédures fermées et à représenter les requérants. Les avocats spéciaux diffèrent des avocats normaux représentant les requérants. Les avocats spéciaux sont autorisés à révéler à leurs clients un résumé simplifié ou un aperçu des éléments de renseignement utilisés dans le cadre d'audiences secrètes, tout en gardant les détails secrets. Les avocats spéciaux doivent défendre les intérêts de ceux qu'ils représentent et peuvent contester la production de certains éléments sur le fondement qu'elle violerait le procès équitable, mais ils ne peuvent pas échanger avec le requérant sans la permission du Gouvernement et ne peuvent jamais révéler de preuves gardées secrètes. » [10]

10. Traduction libre de "*Special advocates are security-vetted lawyers who are permitted to participate in CMPs and represent claimants. Special advocates differ from normal lawyers who represent claimants. Special advocates are permitted to disclose to clients a simplified summary or 'gist' of intelligence material used in secret hearings, while withholding specific details. The special advocates are instructed to protect the appellant's interests and may argue against admitting material on the grounds that it would prevent*

Loin d'être louée, l'institution des avocats spéciaux est ouvertement critiquée, à commencer par la *House of Lords* et par la doctrine britannique, notamment en ce que « l'utilisation des procédures secrètes peut empêcher les requérants d'avoir connaissance de toutes les allégations qui sont faites à leur encontre, ce qui a été critiqué en ce que les parties ne seraient plus sur un pied d'égalité » [11].

Si l'équilibre des parties est considéré comme indûment rompu là où les parties peuvent être représentées par une personne habilitée, alors qu'en est-il de la situation où le justiciable ne peut pas être représenté par une personne habilitée ? *A fortiori*, la rupture n'en est que plus grande. Étant encore une fois précisé qu'il ne s'agit pas que de l'accès aux pièces du procès mais aussi de l'accès aux arguments de la partie adverse et enfin de l'accès au référentiel juridique qui permettra d'apprécier la légalité des mesures dont les justiciables pourraient faire l'objet.

Et le fait qu'aux termes de l'article L. 773-5 CJA, le juge administratif soit en mesure de soulever tout moyen d'office ne peut en rien compenser cette aveuglement de la défense. Le juge aura beau soulever tout moyen, son office n'est pas d'assurer la défense d'une des parties mais uniquement de juger de la légalité des mesures qui sont portées à son attention.

Le déséquilibre profond et disproportionné qui entache la procédure créée par les articles L. 773-1 CJA et suivants est d'ailleurs confirmé par la lecture de la décision *Kennedy contre Royaume-Uni* du 18 mars 2010 de la Cour européenne des droits de l'homme (affaire n° 26839/05). Dans cette affaire, la CEDH a « souscrit à la thèse du Gouvernement [britannique] selon laquelle la divulgation de documents écrits et la désignation d'avocats spéciaux étaient impossibles en ce qu'elles auraient empêché la réalisation de l'objectif poursuivi, à savoir la préservation du secret sur la réalisation d'interceptions. » Mais il est à relever que si la Cour a considéré la procédure qui lui était déférée comme conforme à l'article 6, paragraphe 1 de la CESDH, ce n'est qu'après avoir relevé que « lorsque la CPE [le « *Investigatory Powers Tribunal* »] donne gain de cause à un plaignant, il lui est loisible de divulguer les documents et les informations pertinents en application de l'article 6.4 de son règlement ». Soit une possibilité qui représente un minimum pourtant absent dans la procédure ici instituée.

Il était pourtant loisible de compenser l'inaccessibilité du requérant aux audiences à huis clos et aux écritures secrètes produites par l'administration en créant un « ordre d'avocats spéciaux » jouissant d'un accès spécial aux procédures contentieuses liées aux abus des services de renseignement et chargés de la défense des requérants [12].

---

a fair trial, but they may not communicate with the appellant without the government's permission and they can never communicate about the secret evidence" `http://www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU%282014%29509991_EN.pdf`, p. 22)

11. Traduction libre de "*The use of CMPs might prevent claimants from being aware of all the allegations made against them, which has been criticised on the grounds that parties are no longer on an equal footing.*", J. Jackson (2013), "*Justice, Security and the Right to a Fair Trial : Is the Use of Secret Evidence Ever Fair ?*", Public Law, 720-736, cité in id., p. 23).

12. Il est d'ailleurs à noter que le principe d'un accès privilégié de certains avocats aux procédures administratives n'est pas étranger au Conseil d'État.

11.3.2. La justice pénale entravée par le secret

À cette rupture d'égalité, s'ajoute le fait que lorsque le Conseil d'État constate une illégalité, l'article L. 773-7 alinéa 3 ne prévoit aucune transparence :

> *« Lorsque la formation de jugement estime que l'illégalité constatée est susceptible de constituer une infraction, elle en avise le procureur de la République et transmet l'ensemble des éléments du dossier au vu duquel elle a statué à la Commission consultative du secret de la défense nationale afin que celle-ci donne au Premier ministre son avis sur la possibilité de déclassifier tout ou partie de ces éléments en vue de leur transmission au procureur de la République ».*

Or, en France, la déclassification de documents reste une prérogative exclusivement gouvernementale. Même lorsque la Commission consultative du secret de la défense nationale, saisie par le Conseil d'État, se déclarera favorable à la déclassification en vue de faire la transparence sur les situations d'illégalité constatées et permettre ainsi des poursuites pénales, le Premier ministre, à la fois juge et partie, pourra s'y opposer.

En conclusion,

Il ressort des développements de la présente section que les dispositions des articles L. 773-1 et suivants du code de justice administrative portent atteinte de manière disproportionnée au principe de l'existence d'une procédure juste et équitable garantissant l'équilibre des droits des parties.

Pour assurer *a minima* le respect des droits de la défense, le législateur aurait dû octroyer au Conseil d'État un pouvoir de déclassification des documents secret-défense soumis par l'administration au cours de la procédure dès lors qu'il estime que le secret n'est pas justifié, afin que ces pièces puissent être transmises au requérant ou, le cas échéant, au procureur. Dans tous les cas, les audiences en huis clos prévues par l'article L. 773-4 apparaissent contraires à l'équité du procès.

Faute de réserves d'interprétation à cet effet, les dispositions concernées devront être censurées ainsi que l'essentiel des pouvoirs octroyés à l'administration, puisque ces derniers ne pourront alors plus faire l'objet de recours contentieux. Dans un tel cas, il appartiendrait au législateur d'adopter un nouveau texte pour s'assurer que les dispositions du code de la sécurité intérieure dans le champ du renseignement, et en particulier la procédure contentieuse prévue en la matière, respectent pleinement les droits et libertés constitutionnellement garantis.

Cinquième partie

DIVERS

12. Cavalier législatif

12.1. L'aggravation des sanctions prévues pour les délits de fraude informatique constitue un cavalier législatif

En droit,

Depuis une décision du 10 juillet 1985, le Conseil constitutionnel s'assure que les amendements adoptés ne sont pas dépourvus de tout lien avec les dispositions figurant dans le projet de loi initial. Dans le cas contraire il s'agit de « cavaliers législatifs ». Ce contrôle, dont l'ancrage constitutionnel est consacré avec la décision n°199-DC du 28 décembre 1985 (cons. 2.), découle du premier alinéa des articles 39 et 44 de la Constitution.

En l'espèce,

La loi déférée comporte un article 4, introduit par un amendement du rapporteur du texte à l'Assemblée nationale, qui dispose :

> ***Article 4***
> *« Le code pénal est ainsi modifié :*
> *« 1° L'article 323-1 est ainsi modifié :*
> *a) Au premier alinéa, le montant : « 30 000 euros » est remplacé par le montant : « 60 000 € » ;*
> *b) Au deuxième alinéa, le montant : « 45 000 euros » est remplacé par le montant : « 100 000 € » ;*
> *c) Au dernier alinéa, le montant : « 75 000 € » est remplacé par le montant : « 150 000 € » ;*
> *« 2° L'article 323-2 est ainsi modifié :*
> *a) Au premier alinéa, le montant : « 75 000 euros » est remplacé par le montant : « 150 000 € » ;*
> *b) Au second alinéa, le montant : « 100 000 € » est remplacé par le montant : « 300 000 € » ;*
> *« 3° L'article 323-3 est ainsi modifié :*
> *a) Au premier alinéa, le montant : « 75 000 euros » est remplacé par le montant : « 150 000 € » ;*
> *b) Au second alinéa, le montant : « 100 000 € » est remplacé par le montant : « 300 000 € » ;*

« 4° À l'article 323-4-1, le montant : « 150 000 € » est remplacé par le montant : « 300 000 € ». »

En séance à l'Assemblée nationale, le 15 avril dernier, le ministre de la Défense avait émis un avis défavorable à l'adoption de cet amendement :

> **M. Jean-Yves Le Drian**, *ministre*. Cet amendement a déjà été déposé et adopté par votre assemblée au cours des débats préalables à la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme. Toutefois ces dispositions n'avaient pas été adoptées par le Parlement en raison de l'hostilité du Sénat, pour qui cette augmentation très sensible des peines d'amende rompait l'échelle habituelle des peines ainsi que la cohérence entre les plafonds d'amende et les peines d'emprisonnement encourues. Nous pouvons d'ailleurs observer que les peines d'amende sont déjà particulièrement sévères lorsque les faits modifient les données du traitement mis en œuvre par l'État – l'amende est alors de 100 000 euros – ou lorsque ces faits sont commis en bande organisée et vont à l'encontre du traitement mis en œuvre par l'État – elle s'élève alors à 150 000 euros.
>
> **Je rappelle par ailleurs que ces dispositions sont sans lien avec le renseignement.**
>
> Pour toutes ces raisons, le Gouvernement émet un avis défavorable.

En conclusion,

Cet article vise à une aggravation des peines pour les délits informatiques [1], sans rapport avec l'objet initial du texte, à savoir les techniques de renseignement et leur encadrement. Comme l'a lui-même relevé le gouvernement en séance, il s'agit d'un cavalier législatif.

L'article 4 doit donc être censuré.

1. L'article 4 de la loi déférée a été adopté quelques mois seulement après l'adoption de l'article 17 de la loi de novembre 2014 relative à la lutte contre le terrorisme, qui permet la répression de la fraude informatique commise « en bande organisée ». Ce nouveau fondement est d'ores et déjà utilisé dans le cadre de poursuites pénales intentées contre des militants politiques accusés d'avoir rendu momentanément inaccessibles les sites Internet du conseil régional de Lorraine, du conseil général de la Meuse, et de l'Agence nationale pour la gestion des déchets radioactifs, dans le cadre d'une campagne de la société civile contre les risques nucléaires. Voir : Félix Tréguer, Le droit pénal de la fraude informatique, nouvel ami des censeurs ?, *La Revue des droits de l'homme - Actualités Droits-Libertés*, 2 juin 2015. Disponible à l'adresse : `https://revdh.revues.org/1328` ; Isabelle Rimbert, Une cyberaction pour protester contre le meurtre de Rémi Fraisse pourrait mener des Anonymous en prison, *Reporterre*, 9 juin 2015. Disponible à l'adresse :`http://www.reporterre.net/Une-cyberaction-pour-protester-contre-le-meurtre-de-Remi-Fraisse-pourrait-mener`.