Document 1 de 1

La Semaine Juridique Administrations et Collectivités territoriales n° 40, 5 Octobre 2015, 2286

La loi relative au renseignement : un État de surveillance ?

Etude rédigée par : Xavier Latour
professeur de droit public à l'université de Nice - Sophia Antipolis, CERDACFF (EA 7267)
secrétaire général de l'Association française de droit de la sécurité et de la défense

Sommaire

La loi n° 2015-912 du 24 juillet 2015 relative au renseignement s'inscrit dans un contexte troublé. Sans être une loi d'exception, elle est exceptionnelle. Présentée comme étant l'une des réponses apportées par l'État à la sauvegarde des intérêts fondamentaux de la Nation, et à la lutte contre le terrorisme en particulier, elle autorise les services de renseignement à utiliser des outils tellement importants et critiqués au regard de la protection de la vie privée que le président de la République a saisi le Conseil constitutionnel. Le texte renforce les pouvoirs de police administrative des services de renseignement, tout en essayant de mettre en oeuvre des contrôles de leur fonctionnement en adéquation avec les exigences d'une démocratie. Le tout constitue un nouveau Livre VIII intitulé « Du renseignement » dans le Code de la sécurité intérieure (CSI).

1. - Quelques semaines après les attentats de janvier 2015 et sous le pilotage direct du Premier ministre, le Gouvernement présentait en Conseil des ministres, le 19 mars 2015, un projet ambitieux marqué par une dimension interministérielle (Intérieur, Défense, Justice). Pour une fois et en dépit des apparences, la loi n'a pas été dictée par l'émotion des circonstances ; elle est, au contraire, le résultat d'une réflexion murie. Ses promoteurs ont été guidés par une double exigence dans le domaine de l'accès et du traitement des informations acquises par des services spécialisés ayant « *pour objet de permettre aux plus hautes autorités de l'État, à notre diplomatie, comme aux armées et au dispositif de* ***sécurité intérieure*** *et de sécurité civile, d'anticiper et, à cette fin, de disposer d'une autonomie d'appréciation, de décision et d'action* »[Note 1].

D'une part, notamment sous l'impulsion du député Urvoas et d'une partie de la doctrine[Note 2], la France modernise le cadre légal applicable aux services de renseignement. Déjà, pendant la campagne présidentielle, Monsieur Urvoas avait dessiné les contours d'une politique du renseignement tenant compte des exigences des démocraties[Note 3]. Sur ce point, le changement de majorité a permis de réelles avancées. D'abord, les services de renseignement[Note 4] sont désormais énumérés par un texte, l'article D. 1122-8-1 du Code de la défense. Il s'agit de : la direction générale de la sécurité extérieure (DGSE), la direction de la protection et de la sécurité de la défense (DPSD), la direction du renseignement militaire (DRM), la direction générale de la **sécurité intérieure** (DGSI), la direction nationale du renseignement et des enquêtes douanières et du service à compétence nationale dénommé « traitement du renseignement et action contre les circuits financiers clandestins » (TRACFIN). Ensuite, sur le fondement de la loi de programmation militaire (LPM) n° 2013-1168 du 18 décembre 2013, la délégation parlementaire au renseignement[Note 5] a été renforcée pour mieux contrôler l'action du gouvernement en la matière. Enfin, le décret n° 2014-833 du 24 juillet 2014 crée l'inspection des services de renseignement. Ces réformes amplifient le mouvement amorcé dans les années 1980 de publication des textes relatifs au fonctionnement des services concernés[Note 6].

D'autre part, le texte ouvre aux services de renseignement de nouveaux moyens pour préserver les intérêts fondamentaux de la Nation et de la défense (*CSI, art. L. 811-1*). Cela s'inscrit dans le prolongement des derniers Livres blancs sur la défense et la sécurité nationale qui insistent sur « la connaissance et l'anticipation ». Jusqu'à présent, les prérogatives de surveillance valaient surtout dans le cadre judiciaire. Malgré une accélération législative ces dernières années, les pouvoirs détenus à des fins de surveillance préventive étaient mal définis et peu encadrés. En dépit de plusieurs lois votées entre 2012 et 2014 (sans même évoquer les textes plus anciens), les services de renseignement regrettaient un vide juridique. La loi de 2015 prouve qu'ils ont été entendus et accentue une tendance à la surveillance préventive des populations. Après la loi n° 2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme, la LPM de 2013 a inséré dans le CSI des dispositions discutées sur la surveillance des données de connexion et la géolocalisation en temps réel. Un an plus tard, la loi n° 2014-1353

du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme a concrétisé la volonté du législateur de développer les compétences de police administrative de contrôle des sites djihadistes[Note 7].

Dense, voire compliquée, la loi ne laisse pas indifférent.

D'abord, comme pour plusieurs textes intéressant la sécurité, le consensus politique a globalement prévalu, mais moins que sur d'autres textes. Des critiques sont venues de part et d'autre de l'hémicycle, en transcendant les clivages. Parallèlement, les débats ont été vifs à l'extérieur du Parlement, ce qui tend à démontrer que la démocratie trouve d'autres voies pour s'exprimer. Les dangers réels ou supposés du texte ont été maintes fois dénoncés. Même le *New York Times*, dans un éditorial du 31 mars 2015, titrait « *The French Surveillance State* » quand, dans le même temps, les États-Unis encadrent davantage la collecte des données (*Freedom Act* du 3 juin 2015). Le commissaire aux droits de l'homme du Conseil de l'Europe craignait, quant à lui, dans un communiqué du 19 mars 2015, la multiplication de mesures aux « effets liberticides ». Le Comité des droits de l'homme de l'Organisation des Nations unies était sur une ligne comparable, en juillet 2015. En France, Monsieur Jean-Marie Delarue, président de la Commission nationale de contrôle des interceptions de sécurité (CNCIS) était aussi inquiet[Note 8]. En contradiction avec une sérieuse préparation en amont du projet, le recours à une procédure accélérée a provoqué le sentiment d'un débat tronqué au nom d'impératifs de sécurité. Dans un temps court, les quelques parlementaires présents dans l'hémicycle ont, malgré tout, fait substantiellement évoluer le texte en direction de garanties accrues.

Ensuite, et bien que le gouvernement s'en défende, la loi peut donner l'impression de favoriser le développement d'une surveillance de masse déclenchée par une autorité politique, le Premier ministre. Certaines des techniques autorisées évoquent des pratiques dénoncées lorsqu'elles sont utilisées à l'étranger. Au nom de la détection des menaces, des technologies intrusives dans la vie privée sont mobilisées (interception de sécurité, accès aux données de connexion, captation d'images et de son, y compris grâce à un accès aux réseaux des opérateurs de télécommunication...).

Enfin, la loi innove quant au contrôle des activités de renseignement. En raison de la mise à l'écart du juge judiciaire en matière de police administrative, le texte privilégie la voie d'un contrôle mixte, car administratif en passant par l'intervention d'une autorité administrative indépendante (la commission nationale de contrôle des techniques de renseignement - CNCTR), et juridictionnel grâce à l'intervention du juge administratif.

La loi relative au renseignement est un élément de plus à ajouter au débat classique et inépuisable sur les relations entre la liberté et la sécurité, au point qu'il est légitime de se demander si le juriste et le citoyen ne se sont pas confrontés à une aporie juridique. Le texte reflète la conciliation délicate entre l'action des services et le respect des obligations constitutionnelles (article 2 de la Déclaration des droits de l'homme), autant que conventionnelles (conciliation entre l'ingérence et le droit au respect de la vie privée prévu à l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales). Dès le premier article du nouveau Livre VIII[Note 9], le rappel solennel des principes (en particulier celui de proportionnalité) guidant l'action des services dans le respect de la liberté n'emporte pas la conviction des détracteurs du texte. Ils soulignent d'ailleurs que le caractère exceptionnel de la surveillance prévu pour les interceptions de sécurité dans la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie de communications électroniques, a disparu. Il est vrai cependant que les pratiques de communication ont changé et que le droit devait s'adapter.

Contrairement à la plupart des lois précédentes et pour la première fois de la Cinquième république, le Conseil constitutionnel a été saisi par le président lui-même[Note 10], par plusieurs députés de tous les bords (sauf le Parti socialiste), et par le président du Sénat. Cette saisine novatrice n'a pas été suivie d'une décision audacieuse. En effet, la loi a été très largement validée par le Conseil[Note 11] dans une décision plus ou moins argumentée.

Alors que la loi renforce substantiellement la surveillance préventive (**1**), il n'est pas évident que les garanties prévues suffisent à accompagner ce mouvement (**2**).

1. Le renforcement de la surveillance préventive

2. - Le renforcement passe d'une part, par le champ d'application de la loi. Non seulement les services de renseignement pourront s'appuyer sur une liste de finalités assez large, mais encore ils sont plusieurs à pouvoir prétendre utiliser les prérogatives de surveillance (**A**). D'autre part, les moyens mobilisables sont de plus en plus importants (**B**).

A. - Les services concernés

3. - Sur le fondement de l'article L. 811-2 du CSI, les six services constituant la communauté du renseignement au sens de l'article D. 1122-8-1 du Code de la défense ont vocation à bénéficier des prérogatives précisées par la loi. Le décret en Conseil d'État en fixant la liste devrait logiquement les reprendre.

Cela ne soulève pas d'objection particulière pour les services civils (la DGSI, la douane et TRACFIN). En revanche, l'inclusion des services militaires (DRM et DPSD) et de la DGSE mérite attention. La DGSE n'a normalement pas vocation à intervenir

sur le territoire national, cette compétence relevant de la DGSI.

Alors que le cas de la DPSD est plus compréhensible puisqu'elle protège notamment les industries de défense, celui de la DRM est à rapprocher de la DGSE. Tous les services devaient-ils être traités de la même façon ? Est-il normal de conférer des moyens identiques à des services qui n'ont pas tous la même culture de l'enquête ?

Dans son avis sur le projet de loi, le Conseil d'État écarte rapidement les possibles objections en se contentant de préciser que chaque service « *ne pourra invoquer que des finalités entrant dans le champ de ses missions* »[Note 12], ce que la loi reprend à l'article L. 811-3 du CSI. Il reste à savoir comment ces dernières seront interprétées, alors que, selon la loi, les services agissent pour la « défense » et pour la « promotion » des intérêts fondamentaux de la Nation[Note 13].

Afin de consolider l'action des services, la loi garantit l'anonymat des agents dans les procédures administratives[Note 14], leur accorde une excuse pénale pour des actions commises vers l'extérieur à partir de la France[Note 15] et prévoit une protection juridique adaptée pour des faits d'enquête (contact avec des suspects) commis dans l'exercice de leur fonction[Note 16] ou hors du territoire[Note 17].

La première liste pouvant ne pas suffire, il est prévu d'élargir les bénéficiaires des prérogatives de surveillance à un deuxième cercle de services. L'autorisation d'utilisation ne pourra alors concerner que certaines techniques et finalités[Note 18], sur le fondement d'un décret en Conseil d'État pris après avis de la CNCTR.

Malgré des hésitations, cela ne concernera pas l'administration pénitentiaire[Note 19]. Si l'utilité d'une meilleure connaissance des comportements en prison pouvait motiver le renforcement des moyens de contrôle, cette évolution s'est heurtée à l'opposition de la ministre de la Justice. Selon elle, un développement du renseignement pénitentiaire aurait brouillé la distinction entre le ministère de l'Intérieur et celui de la Justice. Dès lors, les services compétents seront appelés à travailler conjointement avec l'administration pénitentiaire.

En revanche, l'élargissement devrait bénéficier au service central du renseignement territorial rattaché à la direction centrale de la sécurité publique, à la sous-direction à l'anticipation opérationnelle de la gendarmerie nationale et à la direction du renseignement de la préfecture de police de Paris.

Pour agir, les services de renseignement devront poursuivre des finalités textuellement énumérées et plus nombreuses que celles antérieurement prévues à l'article L. 241-2 du CSI à propos des interceptions de sécurité. En étant la première garantie contre d'éventuels abus ou, au contraire, le fondement d'une surveillance élargie, cette liste a été très discutée. Même si les travaux parlementaires ont été marqués par la menace terroriste, les finalités poursuivies sont la préservation[Note 20] :

- de l'indépendance nationale, l'intégrité du territoire et la défense nationale ;

- des intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux et la prévention de toute forme d'ingérence étrangère ;

- des intérêts économiques, industriels et scientifiques majeurs de la France.

Ainsi que la prévention :

- du terrorisme ;

- des atteintes à la forme républicaine des institutions, des violences collectives de nature à porter atteinte à la paix publique, de la reconstitution ou d'actions tendant au maintien de groupements dissous ;

- de la criminalité et de la délinquance organisées ;

- de la prolifération des armes de destruction massive.

La version définitive essaie d'écarter les risques de redondance et d'interprétations abusives. La première version se référait à la sécurité nationale en général (notion particulièrement vague[Note 21]. Les risques d'imprécision et, par voie de conséquence, d'abus ont donné lieu à des modifications qui soulèvent d'autres interrogations. La sécurité nationale est confirmée en sa qualité de stratégie[Note 22] et a été écartée au profit des intérêts fondamentaux de la Nation. Surtout, certaines des expressions retenues pourraient être d'interprétation large. Ainsi, la « *prévention des violences collectives de nature à porter gravement atteinte à la paix publique* » fait craindre une surveillance liée à de simples manifestations. De même, quels seront « *les intérêts majeurs* » de la politique étrangère en sachant que ce qualificatif est nouveau, l'article 410-1 du Code pénal se référant aux « *intérêts fondamentaux de la Nation* », et l'article L. 241-2 du CSI à des intérêts « essentiels » ? De tristes expériences de surveillance à des fins politiques dans un passé pas si lointain incitent à une certaine réserve. Dans ce même registre, le champ d'application de la criminalité et de la délinquance organisées est assez vaste pour susciter des demandes nombreuses. Le Conseil

constitutionnel n'a cependant pas soulevé d'objection sur la précision des objectifs listés.

Malgré une louable volonté de préciser les items retenus, seule leur interprétation permettra de savoir s'il en sera fait un usage restrictif ou extensif.

Conformément aux finalités prévues, les services concernés sont en mesure de mobiliser des moyens inconnus jusqu'alors en matière de police administrative et qui viennent s'ajouter à des moyens existants.

B. - Les moyens mobilisables

4. - La surveillance à des fins préventives s'appuie sur des moyens technologiques toujours plus puissants et intrusifs dans la vie privée. Alors que certaines techniques faciliteront, à juste titre, une surveillance ciblée, d'autres sont, au contraire, associées à une surveillance élargie, parfois qualifiée de masse. Au nom du respect de la vie privée (ce qui comprend la protection des données personnelles), le principe de proportionnalité est censé guider l'usage de ces moyens[Note 23]. Le Conseil constitutionnel prend d'ailleurs soin d'insister sur ce point dans le considérant n° 11 de la décision du 24 juillet 2015.

L'intention du législateur est d'aller au-delà des interceptions de sécurité classiques, issues de la loi n° 91-646, et de l'accès aux données de connexion dans sa version issue de la LPM de 2013. Le droit suit les évolutions technologiques. Il s'adapte aussi aux pratiques de criminels disposant des ressources offertes par les technologies de communication. Les portables jetables, les cybercafés conférant l'anonymat, les logiciels performants de cryptage... sont autant d'instruments utiles à leurs actions.

En ciblant un individu, les services pourront récupérer les données de connexion définies, assez vaguement, à l'article L. 851-1 CSI (ex article L. 246-1 du CSI dont la constitutionnalité a pourtant été confirmée par le Conseil constitutionnel[Note 24]. Elles peuvent être collectées y compris en temps réel en matière de prévention du terrorisme. À cela s'ajoute la localisation d'une personne identifiée comme une menace, soit en temps réel, soit à partir de la reconstitution de ses déplacements (ce qui était déjà possible).

Encore plus attentatoires à la vie privée (mais comment pourrait-il en être autrement ?), les dispositifs de captation, de transmission et d'enregistrement d'images ou de parole dans des lieux privés ou des véhicules sont désormais accessibles aux services de renseignement.

Bien que théoriquement utilisées à l'égard d'individus en particulier, ces techniques auront cependant un impact plus large. Sous l'influence des attentats de janvier 2015, la loi autorise les interceptions de sécurité pour des personnes appartenant à l'entourage d'une personne ciblée et susceptibles de fournir des informations. Le champ d'application des investigations devra, par voie de conséquence, être examiné avec vigilance[Note 25], alors que la CNCIS, créée en 1991, avait tenté de le limiter. La référence à des « raisons sérieuses » de croire que la personne est concernée ouvre une grande marge de manoeuvre.

À l'inverse des précédentes, à rebours des affirmations des promoteurs du texte et de sa lecture par le Conseil constitutionnel, plusieurs techniques semblent favoriser une surveillance élargie. Les capacités de captation de métadonnées sont quasiment aussi intrusives dans la vie privée que la transcription des échanges eux-mêmes. Les métadonnées sont d'ailleurs assimilées à des données personnelles permettant l'identification indirecte des individus, même si les Sages n'en tirent aucune conséquence sur la constitutionnalité de différentes dispositions.

Sur le fondement de l'article L. 851-3 du CSI et à la seule fin de lutter contre le terrorisme, le recours à des algorithmes pour analyser les données de connexion à l'internet a suscité, à juste titre, de nombreuses critiques. Cette technique (curieusement qualifiée de « boîte noire » ou sonde au début des travaux parlementaires) ouvre la voie à une analyse automatisée des comportements sur l'internet pour faire émerger d'un flot de données une menace. La captation de signaux faibles pour leur exploitation implique de collecter très largement des informations. Les développements qui sont consacrés à ces capacités informatiques dans l'étude d'impact sont tellement limités qu'ils n'ont pas rassuré. Face à une méthode d'une grande complexité technique, les critiques se sont multipliées. En plus de l'intrusion massive dans la vie privée, elles ont porté sur les risques de fausses pistes et la difficulté de trier les données strictement nécessaires des autres. Le malaise à l'égard de cette technique est tel que son retrait du texte aurait été justifié. Le brevet de constitutionnalité accordé ne rassure pas, tandis que son évaluation au plus tard le 30 juin 2018 pour une application jusqu'au 31 décembre 2018 (article 25) relève plutôt de la posture, tant les retours en arrière en matière de sécurité sont rares.

Les dispositifs techniques de captation de données téléphoniques par des balises portatives[Note 26] soulèvent des interrogations tout aussi sérieuses. Il s'agit de matériels portatifs de captation des données de connexion nécessaires à l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur. Quand les uns voient une technique circonscrite à un individu suspect, les autres relèvent la captation de données de tout un périmètre.

Dans ces différentes hypothèses, le principe de proportionnalité est-il réellement respecté ? La réponse positive du Conseil constitutionnel serait-elle celle formulée par des juges européens[Note 27] ?

En outre, il conviendra d'observer l'utilisation judiciaire qui sera faite des informations éventuellement transmises sur le fondement de l'article 40 du Code de procédure pénale.

Afin de ne pas entraver les investigations, la loi reprend l'obligation imposée aux fournisseurs de prestations de cryptologie de remettre aux agents des services de renseignement les clés de déchiffrement[Note 28]. Par ailleurs, l'article L. 871-2[Note 29] permet aux autorités compétentes de « requérir » des opérateurs de communications électroniques les informations ou documents qui leur sont nécessaires pour la réalisation et l'exploitation des interceptions de sécurité autorisées par la loi, désormais « *dans les meilleurs délais* ». Il va de soi que ces opérateurs ont l'obligation de ne pas divulguer la mise en oeuvre d'une technique de renseignement[Note 30]. Comment d'éventuels lanceurs d'alerte vivront-ils cette situation ?

Dans un autre registre, l'article L. 561-26 du Code monétaire et financier impose une nouvelle obligation à la charge des transporteurs routier, maritime, ferroviaire et aérien, ainsi qu'aux opérateurs de voyage.

Ils doivent transmettre à TRACFIN, à sa demande, les informations relatives à l'identité, au déplacement et aux bagages des personnes transportées. Les transporteurs routiers ont l'obligation de recueillir l'identité des passagers et de la conserver pendant un an pour les voyages internationaux de plus de 250 km[Note 31]. Destiné à mieux cerner les schémas de financement des activités terroristes et criminelles, ce dispositif interroge. Il suffira, par exemple, de partir d'une ville frontalière pour le vider de son intérêt.

Enfin, conformément aux engagements pris par le Gouvernement après les attentats de janvier 2015, la loi crée un fichier national automatisé des auteurs d'infractions terroristes[Note 32]. Il leur est, par exemple, imposé de déclarer leur domicile tous les trois mois et leurs déplacements à l'étranger. De plus, les agents auront accès au fichier des antécédents judiciaires[Note 33], dans la limite de leurs attributions et pour atteindre les objectifs de l'article L. 811-3 (sauf les points 2 et 3 relatifs à la politique étrangère et aux intérêts économiques).

En quête d'un équilibre incertain entre les limites et les restrictions faites aux libertés, le Parlement et le Gouvernement ont cherché à désamorcer les critiques en mettant en avant les garanties apportées par le texte. Certaines d'entre elles sont incontestables, d'autres sont incertaines.

2. Les incertitudes relatives aux garanties

5. - La loi reprend pour partie des mécanismes applicables à la CNCIS et innove en modernisant le contrôle des moyens de surveillance. Si le texte fixe les bornes applicables à la surveillance (**A**) en organisant son déclenchement et son déroulement, elle prévoit aussi des contrôles *a posteriori* (**B**), en faisant intervenir de manière originale une formation spécialisée du Conseil d'État, en plus de la CNCTR.

A. - Les bornes à la surveillance

6. - L'encadrement des capacités accordées par la loi repose sur deux piliers : d'une part, l'harmonisation des règles applicables aux différentes ressources technologiques ; d'autre part, l'intervention d'une autorité administrative indépendante, la CNCTR qui se substituera à terme à la CNCIS (article 26 de la loi). La CNCTR ne dispose cependant pas du pouvoir d'autorisation puisque celui-ci appartient *in fine* au Premier ministre[Note 34]. Par voie de conséquence, le juge est tenu à l'écart du déclenchement des pouvoirs de police administrative. Ainsi, l'opposition au texte résulte du recours à une nouvelle autorité indépendante au détriment du juge et de la prise de décision par une autorité politique.

La voie suivie est, cependant, classique. Le Premier ministre est l'autorité administrative de principe, seul détenteur du pouvoir de police administrative générale sur l'ensemble du territoire. Il est en charge de l'action du Gouvernement en matière de sécurité nationale[Note 35]. Sa capacité de décision n'a pas à être limitée par une procédure d'avis conforme, cette hypothèse ayant d'ailleurs été écartée dans la loi n° 91-646 sur les interceptions de sécurité.

Dans l'état antérieur du droit, les interceptions de sécurité et la transmission en temps réel des données de connexion (exemple de la géolocalisation) relevaient de la CNCIS et du Groupement interministériel de contrôle placé auprès du Premier ministre[Note 36]. La procédure d'accès aux données de connexion (traces d'une connexion ou d'un appel) impliquait une « personnalité qualifiée » auprès du Premier ministre ou le Premier ministre seul[Note 37], et agissant sous le contrôle de la CNCIS. Dorénavant, la CNCTR est compétente pour l'ensemble des pratiques, conformément aux recommandations du Conseil d'État formulées dans son rapport annuel 2014 sur le *numérique et les droits fondamentaux*.

Les détracteurs du texte ont ciblé leurs critiques sur deux aspects. D'une part, la tendance à recourir à une autorité indépendante conduirait à diluer les responsabilités et serait onéreuse. D'autre part, l'absence d'intervention d'un juge, si possible judiciaire, au regard des méthodes de surveillance intrusives serait inacceptable.

Si la première ne manque pas de fondement, la suivante est discutable. En effet, en interprétant strictement l'article 66 de la

Constitution, le Conseil constitutionnel[Note 38] limite sa portée aux privations de liberté, ce qui conduit à écarter le juge judiciaire. Cela est parallèlement confirmé par la jurisprudence constitutionnelle sur le droit au respect de la vie privée. La vie privée n'étant plus rattachée à l'article 66 de la Constitution mais à l'article 2 de la Déclaration des droits de l'homme, le juge judiciaire n'en est donc pas le garant exclusif[Note 39]. Dès lors, le Conseil constitutionnel a raison d'insister sans ambiguïté (*consid. 18 à 22*) sur la conformité du mécanisme adopté au droit.

Néanmoins, pour contourner les critiques relatives au choix d'une autorité administrative indépendante et celles sur l'absence de juge, le législateur aurait pu être plus imaginatif. Le juge administratif aurait été légitime à intervenir en amont de la décision de police administrative, seul ou en formation collégiale. Bien que sa proximité avec l'administration active soit parfois critiquée, y compris lorsqu'il intervient en référé-liberté, force est de constater qu'il a beaucoup évolué en donnant des gages d'une indépendance garantie par les textes. Cette voie n'a toutefois pas été sérieusement envisagée. Tout en simplifiant le dispositif, elle aurait pourtant permis d'aller un cran plus loin, en admettant qu'à des moyens aussi discutés devait s'appliquer un processus décisionnel novateur. Le juge administratif serait intervenu *a priori*, et pas seulement *a posteriori*, en se passant de l'intervention d'une autorité administrative même indépendante. La pratique dira si le compromis trouvé est satisfaisant.

La création de la CNCTR n'est pas dénuée d'intérêt, au moins en théorie. Son utilité réelle dépendra de sa capacité à rendre des avis négatifs et des suites données par le Premier ministre. Si la CNCIS était en général suivie, rien ne garantit qu'il en ira de même, comme rien ne garantit que la pratique ne variera pas d'un Premier ministre à l'autre.

La CNCTR constitue, d'abord, une autorité collégiale. Cette forme est un progrès par rapport à la « personnalité qualifiée », en limitant les risques liés à l'avis d'un individu isolé. Ensuite, la loi lui accorde des garanties d'indépendance, communes aux autorités de ce type (inamovibilité, règles d'incompatibilité, absence d'instruction...). Son président est d'ailleurs nommé par décret du président de la République parmi l'un des membres du Conseil d'État ou de la Cour de cassation composant le collège. Le Sénat a, en outre, réussi à convaincre l'Assemblée et le Gouvernement de faire entrer la nomination dans le champ de l'article 13 § 5 de la Constitution[Note 40].

De plus, sa composition de 9 membres[Note 41] rassure et ce d'autant plus qu'elle est le résultat d'un consensus. Elle garantit la compétence, l'indépendance, le pluralisme et même la parité, en conciliant un contrôle technique et un contrôle parlementaire, sans porter atteinte à la séparation des pouvoirs, ce que craignait pourtant Monsieur Urvoas. La CNCTR comprend, en effet, deux conseillers d'État (nommés par le vice-président), deux magistrats hors hiérarchie de la Cour de cassation (nommés par le Premier président et le procureur général), quatre parlementaires (deux députés et deux sénateurs), ainsi qu'une personnalité qualifiée nommée par l'Autorité de régulation des communications électroniques et des postes (ARCEP). Le nombre retenu a cependant été discuté, notamment en raison des doutes sur la lourdeur de la structure, alors que des autorités comparables en Europe fonctionnent avec moitié moins de membres et que la CNCIS se contentait de 3 membres.

La CNCTR peut se réunir en formation restreinte (conseillers d'État et magistrat) ou plénière.

En toute logique, tous les membres sont astreints au secret et habilités à accéder à des informations relevant du secret de la défense nationale, ce qui tempère les craintes relatives aux effets contreproductifs d'une recherche de transparence peu compatible avec le domaine d'intervention. Si des doutes ont été émis sur la disponibilité des parlementaires, il leur reviendra de prouver leur implication dans le champ du contrôle. À ce titre, l'expérience de la délégation parlementaire au renseignement est plutôt rassurante. En revanche, des incertitudes existent quant à la capacité réelle de la CNCTR à appréhender des sujets d'une grande complexité technique malgré les liens établis avec l'ARCEP.

Enfin, ses moyens devraient être consolidés par rapport à ceux de la CNCIS. Quand celle-ci comptait trois membres et disposait de quatre agents à temps plein, la CNCTR reprendra les effectifs de la précédente et bénéficiera de ceux qui étaient octroyés à la « personnalité qualifiée ». La prudence s'impose toutefois. Avant sa censure par le Conseil constitutionnel (cons. 47) en raison de l'empiètement sur le domaine de la loi de finances, l'article L. 832-4 du CSI garantissait théoriquement les moyens de la CNCTR. Il était pourtant déjà possible de s'interroger sur ses capacités financières, techniques et humaines d'accomplir ses missions. Les doutes augmentent après la censure, même si le législateur peut y remédier assez aisément. Les ressources octroyées permettront-elles réellement à la CNTCR de travailler sereinement, surtout si les demandes sont nombreuses ? Dans son rapport pour l'Assemblée nationale, Monsieur Urvoas ne dissimulait pas son trouble, en soulignant la faiblesse de l'étude d'impact sur ce sujet[Note 42]. Parce que les autorités indépendantes ne le sont pas budgétairement, un gouvernement pourra être tenté de réduire les capacités d'action de la CNCTR en réduisant son budget.

La transformation de la CNCIS en CNCTR est indissociable de la nouvelle procédure d'autorisation du recours aux moyens de surveillance. En s'inspirant de la procédure qui était suivie par la CNCIS et conformément au principe de prévisibilité de la loi, le législateur avait créé une procédure unique de droit commun, une procédure renforcée, une procédure d'urgence et une procédure spécifique pour les communications internationales.

Validée par le Conseil constitutionnel, la procédure de droit commun permettant à un agent individuellement désigné et habilité d'agir[Note 43] repose sur la consultation de la CNCTR. Elle est le préalable à l'autorisation délivrée par le Premier ministre en réponse à une demande motivée d'un service et transmise par le ministre de tutelle ou un collaborateur direct habilité au secret

de la défense nationale[Note 44]. Malgré une demande formulée par Monsieur Urvoas en Commission mixte paritaire, la dispense de consultation de la CNCTR pour la surveillance d'une personne (française ou étrangère) ne résidant pas habituellement en France a été écartée. Il aurait été regrettable de créer un dispositif à deux vitesses, tout en tenant un discours sur le renforcement des droits, même si, juridiquement, la rupture du principe d'égalité pouvait se discuter.

En contrôlant la proportionnalité de la mesure de surveillance demandée aux circonstances, la CNCTR éclairera l'autorité politique dans un délai de 24 heures. Pour des raisons pratiques et en l'absence de difficulté, l'avis peut être donné par un seul membre de la Commission (magistrat ou conseiller d'État). Cette façon de procéder nécessitera de fixer des lignes directrices afin d'éviter les divergences d'appréciation. En cas de doute, le collège peut être réuni et rend alors son avis dans un délai de trois jours. Dans les deux cas, les délais fixés paraissent compatibles avec les nécessités de l'action.

Sans doute dans ce but, le silence gardé vaut acceptation[Note 45]. Pour des décisions lourdes de conséquences pour les libertés, une réponse explicite aurait été préférable et plus conforme à la jurisprudence du Conseil constitutionnel. En d'autres temps, au nom des risques pour les libertés, il avait censuré une disposition de la loi n° 1995-73 d'orientation et de programmation relative à la sécurité qui assimilait le silence à une acceptation pour l'installation de caméras de vidéosurveillance[Note 46].

Sur le fondement de l'article L. 821-4 du CSI, le Premier ministre accorde, en principe, une autorisation motivée et circonstanciée, pour une durée maximale de 4 mois, renouvelable dans les mêmes conditions que la délivrance initiale. Les demandes et les autorisations délivrées sont archivées dans un registre centralisé au nom d'un principe de traçabilité et pour faciliter les contrôles de la CNCTR.

La procédure renforcée concerne les atteintes les plus marquées à la vie privée.

Il s'agit, d'une part, des algorithmes et des balises de captation des données d'appel à partir de téléphones portables. Les algorithmes[Note 47] sont employés uniquement pour la prévention du terrorisme. Tout en insistant sur le respect du principe de proportionnalité, la loi limite l'autorisation à une durée de 2 mois renouvelable. Les paramètres retenus doivent être explicités, ce qui renforce la motivation. En outre, ils ne sont pas conçus pour l'identification immédiate des personnes. Seule une autorisation du Premier ministre, après avis de la CNCTR ouvrira cette faculté. Dans ce cas, l'exploitation des données avant destruction doit se faire dans un délai de 60 jours à compter du recueil, sauf en cas de confirmation d'une menace terroriste. Les balises IMSI[Note 48] font, quant à elles, l'objet d'une limitation pour les utilisations simultanées, et d'un registre spécial. Les informations recueillies (terminal utilisé, numéro d'abonnement, données de géolocalisation) sont conservées 90 jours et centralisées par un service du Premier ministre. Alors que la version initiale du projet était plus protectrice des libertés, le champ du procédé a été étendu au-delà du terrorisme pour offrir plus de flexibilité aux services. En revanche, comme pour les interceptions de sécurité[Note 49], le nombre d'appareils utilisés simultanément est contingenté par le Premier ministre[Note 50].

Le renforcement de la procédure s'applique, d'autre part, à la sonorisation de lieux et véhicules, ainsi qu'à la captation d'images et de données informatiques[Note 51]. Sous la pression des parlementaires, ces procédés exigent un avis exprès de la CNCTR en formation collégiale et sont limités à 30 jours d'utilisation (renouvelable) pour la sonorisation de locaux et à 2 mois pour les ordinateurs[Note 52]. En tout état de cause, l'incapacité d'agir autrement doit les justifier[Note 53], ce qui oblige à un effort de motivation.

La procédure d'urgence se dédoublait initialement en urgence absolue et en urgence opérationnelle avant la censure de cette dernière. L'invocation de l'urgence doit, en tout état de cause, être exceptionnelle.

En cas d'urgence absolue[Note 54] applicable à la préservation de l'indépendance nationale, à la lutte contre le terrorisme et à la prévention des atteintes à la forme républicaine des institutions, l'avis de la CNCTR n'est pas requis. Le Premier ministre donne son autorisation, et informe immédiatement la CNCTR dans les 24 heures. Conformément à l'article L. 821-6 du CSI, la CNTR pourra alors se prononcer *a posteriori*, et recommander l'interruption de la mesure, voire saisir le Conseil d'État. Malgré sa mise à l'écart concernant les algorithmes[Note 55], cette procédure ne dissipe pas totalement un sentiment de gêne en raison de la comparaison avec les pratiques de la CNCIS qui était capable de se prononcer à très bref délai.

En cas d'urgence opérationnelle (initialement prévue par l'article L. 821-6 et applicable au balisage d'un véhicule et à l'accès aux données de connexion en temps réel y compris par ISMI), l'action des services ne devait pas être entravée par une procédure trop lourde. « De manière exceptionnelle », l'autorisation du Premier ministre aurait donc été délivrée après déclenchement par un agent individuellement désigné et habilité. Le Premier ministre et la CNCTR auraient été informés sans délai de l'usage de la technique et de ce qui la motivait. Après avis de la CNCTR, le chef du gouvernement aurait pu en prolonger la mise en oeuvre dans un délai de 48 heures ou imposer son retrait et la destruction des données collectées. Ces éléments de procédure n'ont pas été jugés suffisants par les Sages qui ont détecté, pour une fois, une atteinte disproportionnée au droit à la vie privée et au secret des correspondances (*consid. 29*).

Dans le cas de professions protégées, des garanties spécifiques sont prévues. Les avocats, les magistrats, les journalistes et les parlementaires sont exclus de ces procédures[Note 56], sauf s'il existe une raison de penser qu'ils servent de « couverture » à une opération criminelle. Dans ce cas, la CNCTR devra rendre un avis exprès, en formation plénière et être informée du résultat

des transcriptions. La surveillance d'un lieu privé à usage d'habitation est également exclue de l'urgence, en exigeant un avis de la CNCTR.

Enfin, un régime particulier défini par un décret en Conseil d'État après avis de la CNCTR[Note 57] devait s'appliquer aux communications étrangères se rattachant à la France. Cette disposition semblait renvoyer au fonctionnement de la plateforme nationale de cryptage et de décryptement[Note 58] (PNCD) gérée par la DGSE. Des doutes fondés ont émergé à propos de sa possible mutualisation avec les autres services de renseignement, ce que le Premier ministre a fermement démenti, notamment à l'Assemblée nationale, le 13 avril 2015. En tout état de cause, la disposition visée a soulevé la question de la collecte de données personnelles françaises par un service supposé travailler sur des éléments étrangers et qui, de surcroît, échangerait des données avec des services de renseignement étrangers.

Le Conseil constitutionnel a tranché en faveur de la censure en considérant que la loi ne définissait pas les garanties accordées aux citoyens pour l'exercice des libertés publiques (*consid. 78*). Malgré son bienfondé, la décision a aussi pour conséquence de laisser perdurer un vide juridique[Note 59] lequel devrait être comblé par un texte spécifique[Note 60].

Les résultats de la surveillance sont, eux aussi, encadrés[Note 61]. Outre les relevés de mise en oeuvre d'une technique centralisés par le Premier ministre, la durée de conservation varie selon la nature des informations collectées (de 30 jours pour les interceptions de correspondance à quatre ans pour les données de connexion, voire plus pour les données liées à des cyber-attaques et les données cryptées). Si les parlementaires ont été tentés de computer les délais à partir de leur exploitation, ils sont revenus à davantage de sagesse en retenant comme point de départ le recueil. Pour sa part et dans un domaine propice à la subjectivité, le Conseil constitutionnel a validé les durées retenues.

Au final, il va se constituer un vaste réseau de données collectées, circulant entre les services spécialisés, voire au-delà[Note 62]. Dans le contexte de la multiplication des départs de djihadistes à l'étranger, il a en effet paru judicieux d'établir des contacts, en particulier avec les services sociaux dans des conditions précisées par décret en Conseil d'État.

L'incapacité, souvent dénoncée, de l'État à gérer ses fichiers incite à la prudence quant au suivi efficace de toutes ces données. Pour certains, la crainte est accentuée par la mise à l'écart de la Commission nationale informatique et libertés (CNIL). L'association de la CNIL à l'élaboration du décret sur l'organisation du service du Premier ministre chargé de recueillir les informations ou documents n'est qu'une timide avancée obtenue par le Sénat[Note 63]. Devait-il en être autrement ? Pas forcément, si l'on considère que la CNIL est déjà très sollicitée et que la CNTCR est justement créée pour contrôler.

L'encadrement du renseignement ne se limite pas au contrôle en amont des activités de prévention. La loi organise un contrôle *a posteriori* prenant différentes formes.

B. - Le contrôle *a posteriori*

7. - La CNCTR interviendra dans le contrôle de l'activité. Il est à espérer qu'elle jouera pleinement son rôle. La CNCTR n'est pas le seul mécanisme prévu. Le contrôle de la police administrative relevant du juge administratif, c'est au Conseil d'État que la mission a été confiée.

L'activité de contrôle de la CNCTR[Note 64] prend plusieurs formes dont l'effectivité dépendra de l'interprétation que l'autorité se fera de son rôle, notamment en reprenant ou pas les pratiques de la CNCIS.

D'abord et de manière classique, elle exerce une forme de magistrature morale en répondant aux demandes d'avis du Premier ministre et de la délégation parlementaire au renseignement[Note 65], tout en rédigeant des rapports publics[Note 66]. À ce sujet, les travaux parlementaires ont permis d'imposer des éléments précis de contenu du rapport annuel (nombre de demandes d'autorisation présentées et accordées ; nombre de fois où le Premier ministre n'aura pas donné suite aux recommandations de la CNCTR ; nombre de recours à la procédure d'urgence ; nombre de saisines du Conseil d'État par la CNCTR) afin que la littérature produite soit réellement informative[Note 67]. Parallèlement à la CNCTR, la délégation parlementaire au renseignement pourra entendre chaque semestre le Premier ministre sur l'application de la loi, ainsi que les personnes auxquelles il délèguera son pouvoir d'autorisation (article 21 de la loi).

Ensuite, si la CNCTR ne délivre pas d'avis conforme, elle peut saisir le Conseil d'État[Note 68]. Une telle saisine est particulièrement importante lorsque l'autorisation est donnée par le Premier ministre malgré son avis défavorable. La motivation que lui adresse le Premier ministre pour expliquer qu'il ignore son avis négatif, l'aidera sans doute à agir. Dans les cas les plus attentatoires à la vie privée (surveillance dans un lieu privé à usage d'habitation), le gouvernement a opté pour une saisine du Conseil d'État par le président de la CNCTR, un magistrat ou un conseiller d'État, si le Premier ministre passe outre un avis défavorable de la CNCTR. Le Conseil statue dans un délai de 24 heures et, sauf cas de terrorisme, le Premier ministre attend sa réponse[Note 69]. Dans ces différentes hypothèses, la Commission sera invitée à présenter des observations lors de chaque recours intenté contre une mesure de surveillance[Note 70].

De plus, la CNCTR peut émettre une recommandation pour demander l'interruption d'une surveillance et la destruction des

données associées[Note 71]. En cas de désaccord avec les suites données par le Premier ministre, trois membres de la CNCTR peuvent saisir le Conseil d'État. Sur ce point, la discussion parlementaire a fait évoluer le texte en direction d'un assouplissement des conditions de saisine (la majorité absolue était initialement prévue), mais elle n'a pas abouti à véritablement conférer à l'autorité un véritable pouvoir décisionnel. Pourquoi ne pas l'avoir habilité à ordonner la destruction de données inutiles ou illégalement collectées ? Cela aurait crédibilisé son rôle.

Afin d'avoir une vision exacte des pratiques, elle peut exiger du Premier ministre tous les éléments d'information, notamment tout ou partie des rapports de l'inspection des services de renseignement. Elle dispose d'un d'accès permanent et direct aux relevés de mise en oeuvre des techniques de renseignement[Note 72], ou encore aux algorithmes et plus généralement aux données concernées, le tout étant géré par un service du Premier ministre[Note 73] même si la nécessité, pour des raisons de sécurité, d'avoir plusieurs centres de stockage compliquera le travail de contrôle. Elle est, d'ailleurs, habilitée à pénétrer dans les locaux dans lesquels sont centralisées les informations collectées et dans ceux des opérateurs de communication électronique dans lesquels sont mises en oeuvre des techniques de renseignement[Note 74]. Elle bénéficie aussi de l'expertise de l'ARCEP[Note 75]. Parce que la transparence a aussi ses limites, elle n'a pas accès aux informations communiquées par des services étrangers ou par des organismes internationaux, ou qui pourraient lui permettre de connaître l'identité des sources.

En complément des initiatives prises par la CNCTR et sous l'impulsion du député Urvoas, les agents des services de renseignement se sont vus accorder la possibilité de bénéficier du statut de lanceur d'alerte[Note 76]. En cas de violation des règles, la CNCTR saisira le juge pénal conformément à l'article 40 du CPP ou le Conseil d'État, à condition d'avoir des éléments assez solides.

Or, il est loin d'être évident que les personnels disposent des moyens de prouver leurs allégations en étant tenus par les règles du secret de la défense nationale. Le travail parlementaire s'est heurté aux réticences du Gouvernement et n'a pas permis d'accorder des garanties plus solides. Dans ces conditions, les agents seront peut-être tentés de procéder de manière plus radicale pour dénoncer des pratiques illégales. Par ailleurs, comment le principe d'obéissance hiérarchique, très fort dans les services concernés, évoluera-t-il ?

L'intervention du juge administratif est l'autre possibilité pour contrôler les activités de renseignement (l'article R. 311-1 du CJA attribuait au Conseil d'État la compétence de contrôles des actes de la CNCIS). Les articles L. 773-1 et s. CJA sont modifiés pour lui ouvrir la voie du plein contentieux.

Après quelques hésitations, une solution de compromis a été trouvée. Sans satisfaire les tenants de l'intervention du juge judiciaire, elle constitue malgré tout un contrôle juridictionnel. Une formation spécialisée sera normalement compétente, sauf renvoi à la section ou à l'Assemblée siégeant en formation restreinte dans des conditions précisées par décret en Conseil d'État. Ce choix est judicieux, car il garantit l'unité de la jurisprudence.

Tous les membres concernés seront habilités au secret de la défense nationale, ès qualités. Bien que retenue pour préserver leur indépendance à l'égard des services qui n'auront donc pas à enquêter sur eux, cette solution implique d'habiliter un nombre relativement élevé de personnes. Pour certains parlementaires, cela aurait justifié une habilitation personnelle. Ils auront accès aux données conservées au-delà des durées imposées par la loi pour les besoins du contentieux[Note 77].

Le juge administratif pourra être, théoriquement, saisi par tout citoyen. Il faut encore que celui-ci soit déterminé. Car, non seulement il devra saisir préalablement la CNCTR[Note 78], mais surtout il devra suspecter une surveillance par nature secrète et avoir un intérêt à agir (*quid* des homonymes par exemple ?). En la matière, la mise à l'écart des associations interroge[Note 79]. Dans d'autres domaines, elles ont démontré leur capacité à approfondir le contrôle juridictionnel là où des individus hésitent souvent à agir.

S'il est possible de regretter la limitation apportée au respect du contradictoire, la particularité du sujet oblige à certaines concessions à l'origine d'une asymétrie, y compris dans l'accès aux pièces du dossier. Le requérant ne saura rien des éléments le concernant, et devra accorder sa confiance au juge qui aura un accès total aux informations[Note 80]. Sous l'influence du Conseil d'État, cette solution a été préférée à celle consistant à communiquer des éléments aux requérants, tout en limitant l'accès des juges aux données sensibles.

L'encadrement de la publicité des audiences n'est, quant à elle, guère critiquable.

Il reste à savoir comment le temps du juge administratif se conciliera avec celui d'une action de surveillance. Si le référé est prévu[Note 81], le plein contentieux paraît décalé par rapport aux enjeux. Le législateur n'a pas forcé son imagination pour adapter la procédure à une situation particulière, en fixant, par exemple, un délai maximum pour rendre la décision. Quant à l'action en indemnisation, il sera intéressant d'observer l'évaluation des préjudices...

Le contentieux a trait aussi aux questions préjudicielles susceptibles d'être posées par d'autres juges. Conformément à l'article L. 841-1 du CSI, le renvoi se fait à l'initiative de la juridiction saisie (éventuellement à la demande de l'une des parties). Le Conseil statue alors dans un délai d'un mois.

Avec la loi sur le renseignement, la France se veut exemplaire, tout en développant des méthodes de surveillance préventive. Elle poursuit des objectifs d'une manière qui ne satisfera jamais totalement les acteurs du renseignement et les défenseurs des libertés. Les uns regretteront les entraves à leur action, quand les autres dénonceront la violation des droits fondamentaux. Son évaluation à 5 ans rouvrira les débats (article 27 de la loi). Mais, permettra-t-elle d'améliorer les garanties des libertés ? L'obsession sécuritaire annihile aisément le courage des gouvernants à reconnaître leurs erreurs.

À condition de dépasser ces antagonismes, l'observateur retiendra les efforts déployés pour consolider les mécanismes de contrôle. L'existence de faiblesses ne discrédite pas totalement l'ensemble. Au moins sur le papier, la puissance publique donne des gages de prévisibilité du droit. En ce sens, elle se démarque de certains États. La proportionnalité est, quant à elle, plus discutable malgré les affirmations du Conseil constitutionnel.

Mais, la force d'un texte dépend de son application par les autorités. Comment garantir que l'État ne déploiera pas des dispositifs occultes comme d'autres démocraties l'ont fait ? Jusqu'où le citoyen est-il en mesure de lui accorder sa confiance ?

Note 1 *Livre blanc sur la défense et la sécurité nationale, 2008, p. 133.*

Note 2 *Le défi du renseignement : Cahiers de la sécurité n° 13, 2010, INHESJ ; B. Warusfel, Justice et sécurité nationale : l'apport de la loi sur le renseignement, in Cahiers de la sécurité et de la justice n° 31, 2015, p. 69.*

Note 3 *J.-J. Urvoas et F. Vadillo, Réformer les services de renseignement français, Fondation Jean Jaurès, 2011.*

Note 4 *X. Latour, Renseignement (ingénierie institutionnelle), in Dictionnaire encyclopédique de l'État (P. Mbongo, F. Hervouët, C. Santulli), Berger-Levrault, 2014, p. 795*.

Note 5 Créée par la loi n° 2007-1443 du 9 octobre 2007 ; *J.-J Urvoas et J.-P Raffarin, L'activité de la délégation parlementaire au renseignement pour l'année 2014 : AN et Sénat, 18 déc. 2014.*

Note 6 Pour un exemple récent, décret n° 2015-386 du 3 avril 2015 fixe le statut des fonctionnaires de la DGSE.

Note 7 *M. Quéméner, Les nouvelles dispositions de lutte contre la cybercriminalité issues de la loi du 13 novembre 2014 renforçant la lutte contre le terrorisme : AJP 2015, p. 32 ; P. Ségur, Le terrorisme et les libertés sur l'internet : AJDA 2015, p. 160.*

Note 8 Voir le 23e rapport, 2014-2015 de la Commission nationale de contrôle des interceptions de sécurité.

Note 9 *CSI, art. L. 801-1*.

Note 10 *P. Jan, Loi sur le renseignement : la saisine présidentielle doit-elle être motivée : D. 2015, 1047*.

Note 11 *Cons. const., 23 juill. 2015, n° 2015-713 DC : JCP A 2015, act. 707* ; *M. Verpeaux, La loi sur le renseignement, entre sécurité et libertés. À propos de la DC 2015-713, JCP G 2015, 981*.

Note 12 *CE, avis, 12 mars 2015, n° 389754, sur le projet de loi relatif au renseignement : Dr. adm. 2015, alerte 62*.

Note 13 *CSI, art. L. 811-1.*

Note 14 *CSI, art. L. 861-1.*

Note 15 *C. pén., art. 323-8.*

Note 16 *CSI, art. L. 863-1*.

Note 17 *CSI, art. L. 862-1.*

Note 18 *CSI, art. L. 811-4.*

Note 19 Elle dispose d'un état-major de sécurité (*D. n° 2008-689, 9 juill. 2008, relatif à l'organisation du ministère de la Justice et arrêté du 9 juillet 2008 fixant l'organisation en sous-directions de l'administration pénitentiaire*) faisant déjà un peu de renseignement.

Note 20 *CSI, art. L. 811-3.*

Note 21 *B. Warusfel, Les implications juridiques et institutionnelles de la notion de sécurité nationale, in Le droit de la défense et de la sécurité en 2013, (sous la dir. de X. Latour, C. Vallar), PUAM, 2014, p. 17.*

Note 22 *CSI, art. L. 811-1.*

Note 23 *CSI, art. L. 801-1.*

Note 24 *Cons. const., 24 juill. 2015, n° 2015-478 QPC.*

Note 25 *CSI, art. L. 852-1.*

Note 26 Appelé « *IMSI catcher* », *CSI, art. L. 851-6.*

Note 27 Par exemple, *CJUE, 8 avr. 2014, aff. C-293/12 et C-594/12 : RTDE 2015, p. 117, note Sylvie Perrou ; CEDH, 18 sept. 2014, Brunet c/ France. N. Hervieu, Le fichage policier sous les fourches caudines européennes : RDH [en ligne], Actualités Droits-Libertés, mis en ligne le 19 septembre 2014, http://revdh.revues.org/879.*

Note 28 *CSI, art. L. 871-1, ex article L. 244-1.*

Note 29 *Ex article L. 244-2.*

Note 30 *CSI, art. L. 881-1 et 2, ex article L. 245-1 et 2.*

Note 31 *C. transports, art. L. 1631-4.*

Note 32 *CPP, art. 706-25-3 et s.*

Note 33 *CSI, art. 234-4.*

Note 34 *CSI, art. L. 821-1.*

Note 35 *C. défense, art. L. 1131-1.*

Note 36 *CSI, art. L. 243-1 à 11.*

Note 37 *CSI, art. L. 246-3, pour la géolocalisation en temps réel.*

Note 38 *Cons. const, 19 janv. 2006, n° 2005-532 DC, Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers : Journal Officiel du 24 Janvier 2006 ; Rec. Cons. const. 2003, p. 31 ; Cons. const., 27 févr. 2015, n° 2014-450 QPC : JurisData n° 2015-003383 ; JCP A 2015, act. 235.*

Note 39 *V. Mazeaud, La constitutionnalisation du droit au respect de la vie privée : Les Nouveaux Cahiers du Conseil constitutionnel, juin 2015, n° 48, p. 7.*

Note 40 Dans sa décision n° 2015-714 du 24 juillet 2015, le Conseil constitutionnel a logiquement validé l'article unique de la proposition de loi organique n° 2015-911 du 24 juillet 2015.

Note 41 *CSI, art. L. 831-1.*

Note 42 *Rapport n° 2269, 2 avr. 2015, p. 39.*

Note 43 *CSI, art. L. 821-1 et s.*

Note 44 *CSI, art. L. 821-2.*

Note 45 *CSI, art. L. 821-3.*

Note 46 *Cons. const., 18 janv. 1995, n° 94-352 DC, Loi d'orientation et de programmation relative à la sécurité : Rec. Cons. const. 1995, p. 170 ; RFDC 1995, p. 362, note Favoreu.*

Note 47 *CSI, art. L. 851-3.*

Note 48 *CSI, art. L. 851-6.*

Note 49 *CSI, art. L. 852-1, VI.*

Note 50 *CSI, art. L. 851-6, IV.*

Note 51 *CSI, art. L. 853-1 et s.*

Note 52 *CSI, art. L. 853-2, II.*

Note 53 *CSI, art. L. 853-3.*

Note 54 *CSI, art. L. 821-5.*

Note 55 *CSI, art. L. 851-3, V.*

Note 56 *CSI, art. L. 821-7.*

Note 57 *CSI, art. L. 854-1.*

Note 58 V. *Le Monde, 11 avr. 2015.*

Note 59 V. *B. Fauvarque-Causson, Les données et la loi française, in 23e rapport de la CNCIS, 2015, p. 43.*

Note 60 *V. Prop. L. AN n° 3042, 9 sept. 2015, relative à la surveillance des communications électroniques internationales.*

Note 61 *CSI, art. L. 822-1 et s.*

Note 62 *CSI, art. L. 863-2.*

Note 63 *CSI, art. L. 851-1 b).*

Note 64 *CSI, art. L. 833-1 et s.*

Note 65 *CSI, art. L. 833-11.*

Note 66 *CSI, art. L. 833-9.*

Note 67 *CSI, art. L. 833-9.*

Note 68 *CSI, art. L. 833-8.*

Note 69 *CSI, art. L. 853-3-III.*

Note 70 *CJA, art. L. 773-3.*

Note 71 *CSI, art. L. 833-6.*

Note 72 *CSI, art. L. 822-1.*

Note 73 *V.* par ex., *CSI, art. L. 852-1.*

Note 74 *CSI, art. L. 871-4.*

Note 75 *CSI, art. L. 833-11.*

Note 76 *CSI, art. L. 861-3.*

Note 77 CSI, *art. L. 822-2 II.*

Note 78 *CSI, art. L. 833-4.*

Note 79 *CSI, art. L. 841-1.*

Note 80 *CJA, art. L. 773-2.*

Note 81 *CJA, art. L. 311-4-1.*