Délibération n° 2015-078 du 5 mars 2015 portant avis sur un projet de loi relatif au renseignement.

(demande d'avis n° 15005319)

La Commission nationale de l'informatique et des libertés,

Saisie par le Secrétaire Général du Gouvernement, pour le compte du Premier ministre, d'une demande d'avis concernant un projet de loi relatif au renseignement ;

Vu la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, notamment son article 8 ;

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 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 ;

Vu le code de la défense ;

Vu le code monétaire et financier, notamment son article L. 561-26 ;

Vu le code des postes et des communications électroniques ;

Vu le code de procédure pénale ;

Vu le code de la sécurité intérieure ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 11-4°-a) ;

Vu la loi n° 2009-1436 du 24 novembre 2009 pénitentiaire ;

Vu l'ordonnance n° 58-1100 du 17 novembre 1958 modifiée relative au fonctionnement des assemblées parlementaires ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Après avoir entendu M. Jean-François CARREZ, commissaire, en son rapport, et M. Jean-Alexandre SILVY, commissaire du Gouvernement, en ses observations,

Émet l'avis suivant :

Le Secrétaire Général du Gouvernement a saisi, en urgence et pour le compte du Premier ministre, la Commission nationale de l'informatique et des libertés, le 20 février 2015, d'un projet de loi relatif au renseignement.

Ce projet de loi a pour objet d'établir un cadre juridique applicable aux activités des services de renseignement. Il détermine ainsi les principes et les finalités de la politique publique de renseignement ainsi que le régime juridique applicable aux techniques de recueil du renseignement susceptibles de porter atteinte à la vie privée et à la protection des données personnelles. Le contrôle de ces techniques

intrusives est confié à une autorité administrative indépendante ainsi qu'à une juridiction administrative spécialisée relevant du contrôle en cassation du Conseil d'Etat. Le projet contient enfin plusieurs autres dispositions relatives au renseignement, concernant notamment l'anonymat des agents des services spécialisés, certaines sanctions pénales, le renseignement en milieu pénitentiaire et l'extension du droit de communication dont dispose le service à compétence nationale « Tracfin ».

Certaines dispositions du projet de loi intéressant directement la protection des personnes à l'égard des traitements automatisés, la Commission a été saisie pour avis dudit projet, en application des dispositions du a) du 4° de l'article 11 de la loi du 6 janvier 1978 modifiée. Conformément à ces dernières, elle devra également être saisie des décrets d'application qui seront nécessaires à la mise en œuvre de chaque technique de recueil du renseignement prévue par le présent projet de loi.

A titre liminaire, la Commission relève que si le présent projet de loi entend créer un régime juridique spécifique s'agissant de la mise en œuvre de techniques de recueil de renseignement intrusives, l'ensemble des traitements de données résultant de cette collecte reste soumis aux dispositions de la loi du 6 janvier 1978 modifiée.

Sur la portée générale du dispositif envisagé

Le projet de loi a pour objets principaux de définir la politique publique de renseignement, ses principes, les services qui y concourent et de doter ces derniers des moyens leur permettant d'exercer certaines de leurs missions. L'article 1er du projet de loi vise ainsi à modifier la partie législative du code de la sécurité intérieure (CSI), afin d'y ajouter un livre VIII intitulé « Du renseignement », définissant notamment différentes techniques de recueil du renseignement à disposition de ces services, la procédure applicable à leur mise en œuvre et les modalités de leur contrôle. Les dispositions projetées doivent dès lors permettre d'encadrer juridiquement les pratiques des services de renseignement pouvant porter atteinte à la vie privée et d'assurer ainsi la licéité de la collecte de l'ensemble des informations recueillies par l'intermédiaire de ces techniques.

Les services concernés par ces dispositions sont les services spécialisés de renseignement définis par le code de la défense, ainsi que les autres services de l'Etat compétents en matière de sécurité nationale et de sauvegarde des intérêts fondamentaux de la Nation qui pourront, dans des conditions fixées par voie réglementaire, être autorisés à mettre en œuvre des techniques de recueil du renseignement.

Le projet de loi vise, d'une part, à étendre aux services de renseignement l'emploi de moyens déjà autorisés dans la cadre de la police judiciaire et, d'autre part, à autoriser l'usage de nouvelles techniques. Il modifie également de manière substantielle les dispositions actuelles du CSI concernant les accès administratifs aux données de connexion et les interceptions de sécurité.

La Commission souligne que si toutes ces techniques ne revêtent pas la même sensibilité du point de vue du respect de la vie privée, l'ensemble des dispositions

ainsi projetées permettra la mise en œuvre de mesures de surveillance beaucoup plus larges et intrusives que ce qu'autorise le cadre juridique actuel en matière de renseignement. En effet, parmi les nouvelles techniques de recueil du renseignement légalisées ou autorisées, certaines sont susceptibles de conduire à une surveillance massive et indifférenciée des personnes.

De telles atteintes au droit au respect de la vie privée, et notamment de la protection des données à caractère personnel, peuvent être justifiées au regard de la légitimité des objectifs poursuivis et des intérêts en cause. En effet, la sécurité nationale et la sauvegarde des intérêts fondamentaux de la Nation constituent des objectifs nécessaires à la protection de droits et de principes de valeur constitutionnelle et conventionnelle, qui peuvent rendre nécessaires des atteintes au droit au respect de la vie privée. Par ailleurs, les outils nécessaires à l'exercice des missions des services de renseignement doivent être adaptés aux nouvelles formes d'actions des personnes et organismes menaçant ces principes fondamentaux.

Néanmoins, les atteintes portées au respect de la vie privée doivent être limitées au strict nécessaire. Elles doivent être adéquates et proportionnées au but poursuivi et des garanties suffisantes doivent être prévues pour en encadrer et contrôler la mise en œuvre. En ce qui concerne les techniques pouvant conduire à une surveillance massive et indifférenciée, ces garanties devront être particulièrement renforcées.

A cet égard, la Commission relève que le projet de loi vise à encadrer les modalités de collecte de renseignements à partir de certaines techniques, mais n'apporte en revanche aucune modification au régime juridique applicable aux fichiers de renseignement que ces informations alimentent.

S'agissant des techniques de collecte autorisées, des garanties importantes sont prévues dans le projet de loi, au premier rang desquelles figure la définition d'un cadre légal cohérent répondant aux exigences d'accessibilité et de prévisibilité de la loi. La définition précise de la politique publique de renseignement, des missions des services spécialisés de renseignement et des moyens qu'ils peuvent être autorisés à mettre en œuvre à des fins limitativement énumérées participe du respect de ces exigences.

En outre, le projet d'article L. 811-1 du CSI relatif au respect de la vie privée, dans toutes ses composantes, qui rappelle notamment le nécessaire respect du principe de proportionnalité dans toute atteinte portée à ce droit, constitue une disposition essentielle. La Commission estime à cet égard que la mention du droit à la protection des données personnelles, qui constitue une composante fondamentale du droit au respect de la vie privée, devrait être ajoutée à celles du secret des correspondances et de l'inviolabilité du domicile dans la rédaction de cet article.

Le projet de loi instaure également un mécanisme de contrôle administratif et juridictionnel de pratiques qui, pour certaines, échappaient à tout contrôle jusqu'à présent.

Des procédures précises d'autorisation de mise en œuvre des techniques de recueil du renseignement sont ainsi prévues, assorties de mesures permettant de faciliter le contrôle *a priori* et *a posteriori* de leur régularité, tout particulièrement en ce qui

concerne la traçabilité de la mise en œuvre de ces techniques. Une nouvelle autorité administrative indépendante, la Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR), est en outre dotée de pouvoirs de contrôle inédits en la matière. Ces dispositions participent dès lors d'une meilleure protection des libertés individuelles à l'égard des pratiques des services de renseignement que celle offerte par le cadre juridique actuel.

Si la Commission prend acte de l'ensemble de ces garanties, les dispositions du projet de loi intéressant directement la protection des personnes à l'égard des traitements automatisés appellent toutefois les observations complémentaires suivantes de sa part.

Sur les techniques de recueil du renseignement

Le projet de loi prévoit la mise en œuvre de plusieurs techniques de recueil du renseignement, à savoir :

- les accès administratifs aux données de connexion, selon plusieurs modalités ;
- les interceptions de sécurité ;
- les mesures de surveillance internationale ;
- la localisation, la sonorisation, et la captation d'images de certains lieux et véhicules et la captation de données informatiques ;
- les dispositifs techniques de proximité (dits « *IMSI catcher* »).

La Commission relève qu'aucune autre technique de recueil du renseignement intrusive, comme par exemple la collecte de données rendues publiques sur internet ou les réseaux sociaux par les personnes concernées, n'est régie par le présent projet de loi.

Celui-ci prévoit un régime d'autorisation administrative, commun aux différentes techniques de recueil du renseignement utilisées. Cette procédure, prévue aux projets d'articles L. 821-1 et suivants du CSI repose, sauf exceptions, sur les éléments suivants :

- un formalisme strict de la demande d'autorisation formulée par les services (finalités recherchées, techniques envisagées, personnes, lieux ou véhicules ciblés) ;
- un avis préalable de la CNCTR, communiqué au Premier ministre ;
- une autorisation de mise en œuvre par le Premier ministre ;
- un contrôle de la CNCTR sur l'emploi des techniques mises en œuvre ;
- un contrôle juridictionnel *ad hoc* avec la création d'une juridiction spécialisée, soumise au contrôle de cassation d'une formation spécialisée du Conseil d'Etat.

Le projet prévoit enfin certaines conditions d'exploitation des renseignements collectés et, en particulier, les modalités de conservation de ces renseignements, les délais et modalités de leur destruction, une traçabilité rigoureuse de la mise en œuvre des techniques de recueil du renseignement, ainsi que les pouvoirs de contrôle de la CNCTR sur ces opérations.

Sur les évolutions des techniques de recueil du renseignement actuelles

L'article 1er du projet de loi modifie tout d'abord substantiellement le cadre juridique applicable aux techniques déjà existantes, à savoir les interceptions de sécurité et les accès administratifs aux données de connexion.

S'agissant des interceptions de sécurité

Celles-ci sont actuellement encadrées par les articles L. 241-1 à L. 245-3 du CSI, lesquels prévoient un régime strict d'autorisation et des conditions de mises en œuvre particulières. Il est ainsi notamment prévu que le recours à cette technique doit être « *exceptionnel* » (L. 241-2), que l'enregistrement des correspondances interceptées est détruit à l'expiration d'un délai de 10 jours au plus tard à compter de la date à laquelle il a été effectué ou encore que le contrôle de la Commission Nationale de Contrôle des Interceptions de Sécurité (CNCIS) intervient *a posteriori*, l'autorisation ayant été délivrée par le Premier ministre.

Plusieurs modifications de ces dispositions sont prévues dans le projet de loi. Le caractère exceptionnel du recours à cette technique n'est plus mentionné et les correspondances seront dorénavant détruites au plus tard à l'expiration d'un délai porté à un mois à compter de leur première exploitation. Dans la mesure où le projet de loi renforce les modalités de contrôle de ces opérations, ces modifications n'appellent pas d'observation particulière de la Commission.

Par ailleurs, le projet d'article L. 852-1 du CSI dispose que les interceptions de correspondances peuvent être autorisées dès lors qu'elles sont susceptibles de révéler, « *directement ou indirectement* », des renseignements entrant dans les finalités mentionnées à l'article L. 811-4 (nouveau) du même code. La Commission prend acte des précisions apportées par le Gouvernement, selon lesquelles cette disposition permet la mise en œuvre d'interceptions des correspondances d'une personne qui est surveillée, non pour ses propres agissements ou projets, mais parce qu'il s'agit du seul moyen de surveiller une autre personne dite « cible » avec laquelle elle est en relation directe. Au regard du caractère particulièrement intrusif de cette surveillance, elle considère que des garanties spécifiques devraient être prévues. La Commission estime donc que le projet de loi devrait être clarifié sur ce point.

Elle relève par ailleurs que l'autorisation de mise en œuvre d'une interception de sécurité emporte automatiquement recueil des données de connexion. La Commission estime que ce caractère automatique est inapproprié, au regard des enjeux différents soulevés par les données de contenu et les données de connexion, et que seule une appréciation au cas par cas des interceptions pouvant donner lieu à la collecte de données de connexion associées devrait dès lors être prévue.

S'agissant de l'accès administratif aux données de connexion

Les dispositions actuellement en vigueur (articles L. 246-1 à L. 246-5 du CSI) permettent, sous le contrôle *a priori* d'une personnalité qualifiée et *a posteriori* de la CNCIS, la mise en œuvre de cette technique. Les dispositions réglementaires du code des postes et des communications électroniques précisent la nature exacte des informations, principalement techniques, qui peuvent être recueillies. La Commission prend acte que le projet de loi ne modifie pas la formulation des dispositions législatives du CSI et que, par conséquent, les informations concernées ne pourront en aucun cas porter sur le contenu des correspondances électroniques.

La durée de conservation des données de connexion collectées par les services de renseignement est modifiée par rapport au cadre juridique actuel. En effet, alors même que ces données étaient initialement conservées un an, les dispositions réglementaires du CSI prévoient, depuis leur récente modification issue de la loi de programmation militaire, une durée de conservation de trois ans. Le projet de loi prévoit que cette durée soit portée à cinq ans.

Au regard de la sensibilité des informations concernées, la Commission exprime ses réserves sur ce nouvel allongement substantiel de la durée de conservation de ces informations, qui n'exclut d'ailleurs aucunement que les données puissent être conservées au-delà aux fins d'analyse technique.

En tout état de cause, en ce qui concerne ces deux techniques de recueil du renseignement (interceptions de sécurité et accès administratifs aux données de connexion), la Commission estime qu'un décret en Conseil d'Etat devrait en préciser les nouvelles modalités de mise en œuvre. Dans la mesure où les renseignements collectés contiennent nécessairement des données à caractère personnel, elle demande que ledit décret lui soit transmis pour avis.

Sur l'utilisation de techniques de recueil actuellement réservées à la police judiciaire

L'article 1er du projet de loi vise en outre à permettre aux services de renseignement de mettre en œuvre de nouvelles techniques de recueil de renseignement, jusque-là uniquement dévolues aux services de police judiciaire :

- la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou de l'image d'une personne se trouvant dans un lieu privé ;
- la captation, la transmission et l'enregistrement de données informatiques ;
- la localisation en temps réel d'une personne, d'un véhicule ou d'un objet.

La Commission rappelle que, sous réserve des garanties appropriées, il n'existe pas d'opposition de principe à voir doter les services de renseignement de techniques similaires à celles dont bénéficient les services de police judiciaire. Ces derniers ont en effet vu leurs moyens progressivement renforcés afin de s'adapter aux nouvelles formes de criminalités. Le présent projet de loi a, de la même manière, pour objet de définir et de clarifier les moyens à la disposition des services de renseignement.

Pour chacune de ces différentes techniques, le code de procédure pénale (CPP) délimite strictement le cadre juridique dans lequel elles peuvent être mises en œuvre, notamment des points de vue suivants : champ d'application, procédure d'autorisation, modalités d'installation de ces dispositifs, garanties mises en œuvre et conditions d'exploitation des données recueillies par ce biais.

Si la Commission n'entend pas faire une comparaison stricte de ces deux types d'activités (police judicaire et renseignement), au regard de la différence de nature de celles-ci, il lui appartient néanmoins d'évaluer les garanties entourant la mise en œuvre des nouveaux dispositifs prévus par le projet de loi.

À cet égard, la Commission relève que certaines garanties, à l'instar des dispositions du CPP, ont été prévues s'agissant de l'intrusion dans un véhicule ou dans un lieu privé à des fins d'installation de ces nouvelles techniques. Elle s'interroge néanmoins sur l'absence de certaines d'entre elles, pourtant nécessaires aux fins d'assurer un meilleur respect de la vie privée.

Ainsi, s'agissant des techniques mentionnées au projet d'article L. 854-1 du CSI, la Commission relève que la nature exacte des données informatiques qui peuvent faire l'objet d'une captation ainsi que les dispositifs de captation effectivement envisagés (enregistrement des frappes clavier, copies d'écran, enregistrement des données émises ou reçues depuis un périphérique audiovisuel, etc.) ne sont pas précisés, ce qui nuit à la clarté et à la prévisibilité du texte, notamment quant à l'encadrement légal et aux garanties à appliquer.

Elle relève en outre qu'il n'est pas prévu de mesures particulières s'agissant des personnes qui font l'objet, dans le cadre de la mise en œuvre de ces mêmes techniques par les services de police judiciaire, de protections spécifiques en raison de leur statut (avocats, journalistes, médecins, parlementaires, etc.).

S'agissant de la procédure applicable à ces techniques, la Commission observe que des dérogations importantes sont prévues au régime d'autorisation commun, notamment sur la localisation en temps réel.

Or, la Commission rappelle que les dispositifs de géolocalisation sont particulièrement sensibles au regard des libertés individuelles, dès lors qu'ils permettent de suivre de manière permanente et en temps réel des personnes, aussi bien dans l'espace public que dans des lieux privés, comme le montrent d'ailleurs les dispositions protectrices du CPP en la matière. Elle estime que cette caractéristique doit dès lors être prise en compte, selon des modalités adaptées, dans le cadre des missions de police judiciaire comme de renseignement.

À titre subsidiaire, la Commission recommande que le projet d'article L. 851-2-3 relatif à la localisation en temps réel d'une personne, d'un véhicule ou d'un objet, soit inséré au sein du chapitre V du titre V du Livre VIII du CSI, et non au sein du chapitre dédié aux accès administratifs aux données de connexion, afin d'améliorer la lisibilité des dispositions du projet de loi.

Sur l'utilisation de nouvelles techniques de recueil du renseignement

Les mesures de surveillance internationale

L'article L. 853-1 du CSI tel que prévu par le projet de loi prévoit la mise en œuvre de « mesures de surveillance internationale », permettant les interceptions de communications électroniques en provenance ou à destination de l'étranger.

La Commission observe tout d'abord qu'aucune indication sur les techniques précisément utilisées dans ce cadre n'est fournie, tant dans le projet de loi que dans l'étude d'impact.

Elle relève en outre que ces mesures sont soumises à une procédure distincte de celle de la procédure commune prévue aux articles L. 821-1 et suivants du CSI (nouveau). En particulier, ces mesures sont mises en œuvre sur seule autorisation du Premier ministre, sans avis de la CNCTR, dont le contrôle *a posteriori* est limité à la simple formulation de recommandations et d'observations. Dès lors, la Commission considère que les décrets en Conseil d'État auxquels il est fait référence à l'article L. 853-1 précité devront apporter toute précision utile s'agissant notamment des techniques effectivement mises en œuvre et du contrôle de ces dispositifs.

La Commission observe enfin que la mise en œuvre de ces mesures est susceptible de viser, par voie de conséquence, un individu situé sur le territoire national qui serait en relation avec la personne ne se trouvant pas sur le territoire français. Dans ce cas, elle relève que les communications concernées sont conservées et détruites dans les conditions générales prévues pour les interceptions de sécurité.

La Commission relève que le projet de loi n'apporte aucune précision sur la nature exacte des techniques utilisées dans le cadre de cette surveillance à l'international. Elle estime dans ces conditions ne pas être en mesure de se prononcer sur le degré d'atteinte porté à la vie privée et aux libertés des personnes ainsi que sur les garanties à prévoir en conséquence.

Les nouvelles techniques de recueil du renseignement

L'article 3 du projet de loi insère trois nouveaux articles dans le chapitre dédié aux accès administratifs aux données de connexion, relatifs à trois nouvelles techniques de recueil du renseignement.

En premier lieu, l'article L. 851-2-1 du CSI tel que prévu par le projet de loi permet le recueil de la « *totalité des informations et documents* » traités par les opérateurs et relatifs à un ensemble de personnes identifiées comme présentant une menace. Il prévoit en outre que ce recueil est effectué en temps réel, directement sur les réseaux des opérateurs.

La Commission relève tout d'abord que les modalités de recueil (en temps réel et directement sur sollicitation du réseau, sans l'intermédiaire des opérateurs de communications électroniques) constituent une évolution majeure au regard du dispositif prévu à l'actuel article L. 246-3 du CSI. Elle considère que cette nouvelle possibilité est de nature à permettre l'aspiration massive et directe des données par

les agents des services concernés sur les réseaux des opérateurs, par l'intermédiaire de la pose de sondes.

Elle s'interroge en outre sur le périmètre exact des données concernées au regard de la formulation retenue, qui ne correspond pas à celle utilisée aux articles L. 851-1 à L. 851-3 (nouveaux) du CSI. Elle estime dès lors que cette formulation devrait être clarifiée afin de préciser, le cas échéant, que seules les données de connexion peuvent être recueillies sur le fondement de ce nouvel article.

Enfin, dès lors que cette mesure ne concerne pas uniquement une personne identifiée mais est susceptible de concerner un ensemble de personnes « *préalablement identifiées comme présentant une menace* », la Commission observe que seule la prévention du terrorisme, et non les autres intérêts publics mentionnés dans le projet de loi, pourra permettre la mise en œuvre de cette mesure, ce qui constitue une garantie substantielle.

Au regard du caractère particulièrement intrusif de cette technique et de son utilisation à l'insu des opérateurs, sur leurs propres systèmes, la Commission estime que les garanties prévues pour préserver les droits et libertés fondamentaux ne sont pas suffisantes pour justifier une telle ingérence dans la vie privée des personnes.

En deuxième lieu, l'article L. 851-2-2 du CSI tel que prévu par le projet de loi prévoit la mise en œuvre, sur les informations et documents traités par les réseaux des opérateurs, d'un dispositif destiné à caractériser « *sur la seule base de traitements automatisés d'éléments anonymes, la préparation d'un acte de terrorisme* ». Il est néanmoins prévu que l'anonymat des personnes concernées soit levé « *en cas de caractérisation de menace terroriste* ».

Ces dispositifs visent à détecter des signaux dits faibles de préparation d'un acte de terrorisme, à partir de critères pré-établis portant sur les données détenues par les opérateurs. Les « signaux faibles » s'entendent de tendances, de *modus operandi*, ou encore de traces qui risquent d'être illisibles ou non détectables prises isolément, mais qui, rapportés à un ensemble de personnes, mettent en évidence des occurrences révélatrices de certains comportements.

La Commission appelle l'attention du Gouvernement sur la formulation retenue concernant cette disposition : si le traitement automatisé de détection des signaux faibles par les opérateurs n'a vocation qu'à identifier un faisceau d'indices permettant de caractériser une menace terroriste, il n'en demeure pas moins qu'il porte sur des données indirectement ou directement identifiantes et non sur des éléments anonymes, comme le démontre d'ailleurs la possibilité de remonter à l'identité de la personne.

À cet égard, la Commission rappelle que ces traitements devront faire l'objet de formalités préalables, conformément aux dispositions de la loi du 6 janvier 1978 modifiée. Le décret en Conseil d'Etat, pris après avis de la Commission, qui devra préciser les modalités d'application de ces dispositions devra en outre prévoir des conditions de transmission adéquates des données, une fois l'anonymat levé, entre les opérateurs et le service demandeur.

En dernier lieu, le projet d'article L. 891-2 du CSI prévoit la mise en œuvre d'un dispositif technique de proximité (« *IMSI catcher* »). Ce procédé consiste à placer une fausse antenne relais à proximité de la personne dont on souhaite intercepter les échanges électroniques, afin de capter les données transmises entre le périphérique électronique et la véritable antenne relais.

La Commission relève que ce dispositif permettra de recueillir les données de connexion ainsi que, dans certaines conditions, le contenu des correspondances. Il devrait dès lors figurer au sein de la liste des techniques de recueil du renseignement.

Si elle prend acte que des modalités de contrôle spécifiques existent, la Commission relève néanmoins qu'il ne semble pas prévu d'autoriser la mise en œuvre d'un « *IMSI catcher* » dans les conditions énoncées aux projets d'articles L. 821-1 et suivants du CSI et ce, alors même que cette technique est de nature à porter une atteinte particulièrement grave aux libertés individuelles. En effet, un tel dispositif permettra de collecter de manière systématique et automatique des données relatives à des personnes pouvant n'avoir aucun lien ou un lien purement géographique avec l'individu effectivement surveillé, et ce pour tous les intérêts publics mentionnés au projet d'article L. 811-4 du CSI.

Au regard de ce qui précède, la Commission constate que la possibilité de recourir à ces trois nouvelles techniques (sonde, dispositif de détection de « signaux faibles » et « IMSI catcher ») caractérise un profond changement de nature dans les mesures de surveillance légalement autorisées. Il ne s'agit plus seulement d'accéder aux données utiles concernant une personne identifiée comme devant faire l'objet d'une surveillance particulière, mais de permettre de collecter, de manière indifférenciée, un volume important de données, qui peuvent être relatives à des personnes tout à fait étrangères à la mission de renseignement, et parmi lesquelles les services de renseignement devront identifier les données utiles à l'accomplissement de leur mission.

Ce changement a des conséquences particulièrement graves sur la protection de la vie privée et des données personnelles. De telles mesures doivent dès lors être assorties de conditions de mise en œuvre plus précises et de nature à limiter les atteintes à ces droits fondamentaux, d'une part, et de modalités de contrôle effectives et adaptées à la nature de ces atteintes, d'autre part.

A cet égard, la Commission est particulièrement réservée sur l'application d'un seul régime d'autorisation (sonde et « signaux faibles ») et de la seule information du Premier ministre et de la CNCTR s'agissant des « IMSI catcher ». Si le contrôle de la CNCTR a toute sa pertinence pour le recours à des techniques ciblées sur des personnes préalablement identifiées, la Commission estime que sa portée se trouve très fortement atténuée dans le cadre des techniques permettant la collecte d'informations de manière indifférenciée.

Sur le nécessaire renforcement du contrôle de l'exploitation des données

Au regard de ce qui précède, la Commission estime que le projet de loi devrait également contenir des dispositions permettant un contrôle plus strict des conditions d'exploitation des données à caractère personnel ainsi collectées.

Si le projet de loi concerne principalement les modalités de collecte de ces informations et ne modifie pas le régime juridique applicable aux fichiers mis en œuvre par les services de renseignement, la Commission estime que des garanties supplémentaires concernant le contrôle de l'exploitation des données ainsi collectées devraient être prévues afin d'assurer un meilleur équilibre entre protection de la vie privée et exigences de l'ordre public.

En effet, il convient de s'assurer qu'au-delà de leurs seules modalités de collecte, les données soient ensuite traitées conformément au droit à la protection des données personnelles, ce que les garanties entourant la collecte des données dans le cadre des techniques concernées par le projet de loi ne sont pas de nature à assurer. En outre, les traitements de données mis en œuvre par les services spécialisés de renseignement sont susceptibles de contenir des données personnelles recueillies par d'autres canaux que ceux visés dans le projet de loi. En tout état de cause, l'ensemble de ces données doivent être traitées conformément aux dispositions de la loi du 6 janvier 1978 modifiée.

Or, ces fichiers, pourtant pleinement soumis à cette loi, ne font actuellement l'objet d'aucun contrôle permettant de garantir qu'ils sont mis en œuvre dans le respect de la protection des données personnelles et des textes applicables en la matière. Certains fichiers de renseignement peuvent en effet ne pas être soumis au contrôle *a posteriori*, sur place ou sur pièce, de la Commission, en application des dispositions de l'article 44-IV de la loi du 6 janvier 1978 modifiée.

Au regard du renforcement considérable des pouvoirs dévolus aux services de renseignement, la Commission estime que le projet de loi devrait lui permettre d'exercer ses pouvoirs de contrôle sur ces traitements. Un tel contrôle ne porterait évidemment que sur le seul respect des textes ayant autorisé ces traitements et sur les conditions de mise en œuvre globale desdits fichiers, et en aucun cas sur l'activité des services de renseignement ou sur la pertinence et la réalité de telle ou telle information.

Afin de garantir la confidentialité des éléments collectés dans le cadre des missions de renseignement, ce contrôle pourrait être organisé selon des modalités particulières et en coopération notamment avec la CNCTR.

La Commission considère que de tels pouvoirs de contrôle constitueraient une garantie supplémentaire essentielle, conforme aux objectifs poursuivis par le projet de loi et de nature à préserver l'équilibre entre le contrôle des techniques de renseignement et le contrôle des fichiers.

Sur le rattachement du contentieux en matière « de droit d'accès indirect » à la juridiction nationale de contrôle des techniques de renseignement

Le projet de loi prévoit que les personnes pourront saisir une juridiction administrative spécialisée, chargée d'examiner les requêtes concernant la mise en œuvre des techniques de renseignement dont les pouvoirs d'instruction, le déroulement des audiences et la nature des décisions sont précisément définies. Ces spécificités s'appliqueront, dans la même mesure, au Conseil d'Etat au sein duquel une formation de jugement spécifique sera instituée pour l'examen des pourvois en cassation (article 2).

Compte tenu du champ d'application du projet de loi qui n'affecte nullement ses compétences à l'égard des traitements, la Commission estime nécessaire que les dispositions relatives au rôle dévolu à la nouvelle juridiction en ce qu'elles font référence à la « mise en œuvre des traitements », soient clarifiées.

Le projet de loi prévoit également de rattacher aux nouvelles formations de jugement spécialisées le contentieux en matière de droit d'accès indirect, auquel la CNIL est étroitement associée, pour certains fichiers intéressant la « sûreté de l'Etat », dont la liste sera définie par décret en Conseil d'Etat.

A cet égard, la Commission rappelle que le droit d'accès indirect, tel que prévu par l'article 41 de la loi du 6 janvier 1978 modifiée, n'emporte pas un droit à communication des données. En contrepartie de ce régime d'exception, le contrôle du juge administratif porte sur l'appréciation du refus de communication opposé par le responsable du traitement au regard de la sûreté de l'Etat, de la défense ou de la sécurité publique. Ce contrôle peut dès lors avoir pour conséquence d'autoriser la communication desdites données.

Ainsi, alors que les juridictions administratives de droit commun peuvent décider soit du rejet de la requête, soit de l'annulation de la décision de refus de communication des données par le responsable du traitement, les dispositions législatives projetées ne permettront en aucun cas aux nouvelles formations de jugement de confirmer ou d'infirmer, auprès de la personne, la présence de données dans le traitement ».

Dès lors, la Commission considère que le projet de loi marque un recul important par rapport aux garanties apportées par le dispositif actuel s'agissant du droit d'accès aux données. Elle estime qu'en privant les formations spécialisées en ce domaine de tout pouvoir d'appréciation concernant le bien-fondé du refus de communication des données initialement opposé, le projet de loi affecte la protection du droit des personnes.

En outre, si l'objectif principal est de faire en sorte que, contrairement à la jurisprudence actuelle, l'examen par le juge puisse être opéré hors du contradictoire afin de protéger les informations concernées, la Commission estime que le dispositif actuellement en vigueur aurait pu être aménagé en ce sens, à l'instar de ce qui est prévu par l'article 7 du présent projet de loi concernant les actes réglementaires et individuels relatifs à l'organisation et à la situation des agents des services de renseignement spécialisés.

En tout état de cause, la Commission rappelle que ce projet de loi ne saurait la priver ni de sa faculté d'être avisée des recours engagés ni de celle de faire valoir ses observations.

Un nombre important de contentieux est actuellement en cours devant les juridictions administratives de droit commun. La Commission estime dès lors que si ces dispositions devaient être adoptées par le législateur, elles devraient s'accompagner de dispositions transitoires.

Sur les autres dispositions du projet de loi

L'article 8 du projet de loi vise à modifier l'article L. 561-26 du code monétaire et financier afin d'élargir l'étendue du droit de communication des agents de la cellule de renseignement financier nationale (TRACFIN), qui constitue un tiers autorisé à accéder à de nombreuses données à caractère personnel.

Il est ainsi prévu que ces agents puissent obtenir, auprès de toute entreprise de transport (terrestre, ferroviaire, maritime, aérien) ou d'un opérateur de voyage ou de séjour, des éléments permettant d'identifier des personnes ayant payé ou bénéficié d'une prestation ainsi que des éléments relatifs à la nature de cette prestation et s'il y a lieu, aux bagages et marchandises transportées. La Commission observe à cet égard que l'étude d'impact du projet de loi précise que les éléments d'information relatifs à la nature de la prestation rendue ne concernent que « *la date, heure et lieu de départ et d'arrivée* ». Dès lors, elle recommande que cette restriction figure expressément dans le projet de loi.

Par ailleurs, la Commission relève qu'aucune précision n'est apportée quant aux modalités d'exercice de ce droit de communication, alors même que ces précisions apparaissent dans les autres dispositions du même code relatives au droit de communication de TRACFIN.

Au vu des objectifs poursuivis, ces dispositions n'appellent pas d'observations particulières. La Commission rappelle néanmoins que ces accès doivent s'exercer dans les conditions habituelles s'agissant d'un droit de communication, c'est-à-dire sur demande ponctuelle et motivée, portant sur des personnes préalablement identifiées et sans aboutir à la transmission de fichiers entiers ou à des interconnexions de traitements.

L'article 10 du projet de loi modifie enfin certaines dispositions de la loi n° 2009-1436 du 24 novembre 2009 pénitentiaire, notamment en vue de faire face à l'introduction, dans les établissements pénitentiaires, de téléphones portables en contravention des règles prévues par les textes en la matière. Ainsi, l'administration pénitentiaire pourra mettre en place des « *mesures de brouillage, d'écoute ou d'interception* » des correspondances émises ou reçues sur un matériel introduit frauduleusement dans un établissement pénitentiaire, lorsque le maintien de la sécurité et du bon ordre des établissements, la prévention de la récidive ou la protection des intérêts des victimes l'exigent.

D'une manière générale, la Commission estime que la mise en œuvre de mesures de surveillance des matériels introduits de manière frauduleuse dans les établissements pénitentiaires ne soulève pas de difficultés particulières.

Néanmoins, elle relève qu'il n'est pas expressément fait référence, pour ces interceptions ou écoutes, aux techniques utilisées, et notamment aux « *dispositifs techniques de proximité* » prévus dans des dispositions distinctes, et estime que le projet de loi devrait être précisé sur ce point.

En outre, dès lors que le projet de loi prévoit que les personnes nouvellement écrouées seront informées de la mise en œuvre de ces dispositifs, il serait opportun d'uniformiser l'information de l'ensemble des personnes détenues.

L'article 10 du projet de loi permet par ailleurs à l'administration pénitentiaire de mettre en œuvre « *tout dispositif de contrôle, captation, fixation ou enregistrement de données* » permettant de contrôler si le matériel informatique ou tout matériel assimilé sont régulièrement détenus. La Commission rappelle que l'administration procède déjà au contrôle des matériels informatiques détenus par les personnes placées sous main de justice, conformément aux dispositions réglementaires du CPP. Elle prend acte que cette possibilité sera dorénavant prévue dans des dispositions législatives, qui permettront en outre d'installer des logiciels permettant de détecter les connexions frauduleuses.

La Présidente

I. FALQUE-PIERROTIN