La Commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique a souhaité rendre publique une recommandation portant sur le projet de loi relatif au renseignement en cours d'examen au Parlement.

Dans un contexte marqué par les révélations d'Edward Snowden sur la surveillance en ligne massive et généralisée des individus, ainsi que par des menaces terroristes dont l'extrême gravité a été confirmée, la Commission considère que l'actualisation des textes régissant les activités de renseignement est indispensable.

La Commission a procédé à plusieurs auditions sur les activités de renseignement à l'ère numérique. Elle ne méconnait pas les usages des réseaux numériques par les mouvements terroristes. Elle a également pris la mesure de la nouvelle puissance que donnent aux États les technologies de surveillance.

Au moment où les réseaux numériques ont pris une place importante dans la vie des individus, un nombre croissant d'outils technologiques de plus en plus perfectionnés et intrusifs facilite leur exploration par les autorités publiques sans que soit défini un cadre juridique adapté qui en précise les conditions d'utilisation. La Commission souhaite en préalable mettre en garde contre le risque d'aller, pas à pas, d'une surveillance ciblée à une surveillance généralisée.

Il apparaît donc nécessaire de légaliser et d'encadrer les pratiques existantes acceptables. Il convient ainsi de **définir un régime juridique global, cohérent et protecteur des libertés fondamentales pour les activités de renseignement**, ménageant un juste équilibre entre les nécessités constitutionnelles de préservation de l'ordre public – à laquelle les services de renseignement participent – et les droits de chacun au respect de sa vie privée, de sa correspondance, de son domicile et de ses données personnelles.

Ce régime doit être conforme à l'**article 2 de la Déclaration des droits de l'homme et du citoyen de 1789** et à l'**article 8 de la Convention européenne des droits de l'homme et des libertés fondamentales** aux termes duquel il ne peut y avoir ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée et familiale, du domicile et de la correspondance que pour autant qu'elle est prévue par une loi accessible et prévisible et qu'elle est nécessaire, dans une société démocratique, à la poursuite d'un but légitime. La Commission souligne l'importance accordée par la CEDH au caractère prévisible et accessible de la loi, qui « *doit user de termes assez clairs pour indiquer aux individus de manière suffisante en quelles circonstances et sous quelles conditions elle habilite les autorités publiques à prendre des mesures de surveillance secrète* ». Ainsi, la Cour estime que « *les écoutes et autres formes d'interception des entretiens téléphoniques représentent une atteinte grave au respect de la vie privée et de la correspondance. Partant, elles doivent se fonder sur une "loi" d'une précision particulière. L'existence de règles claires et détaillées en la matière apparaît indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner* » .

*

Le projet de loi pose les principes et finalités de la politique publique de renseignement et la procédure d'autorisation des techniques de recueil du renseignement. Il définit la composition, les missions et les prérogatives de l'autorité administrative indépendante qui sera chargée de contrôler la mise en œuvre de ces techniques. Il introduit un recours juridictionnel permettant de contester cette mise en œuvre. Il encadre enfin les conditions dans lesquelles chaque technique de recueil du renseignement peut être utilisée.

(1) Selon le Gouvernement, le projet de loi relatif au renseignement vise à « *mieux encadrer l'activité des services de renseignement* » et à « *donner, par voie de conséquence, un cadre légal à l'activité des services de renseignement en leur permettant d'élargir le spectre légal des techniques pouvant être mises en œuvre, pour mieux répondre aux finalités énoncées par la loi* ». Si la Commission partage ces deux objectifs, elle rappelle que **la légalisation de pratiques de surveillance jusqu'alors peu encadrées ne doit pas être l'occasion d'étendre à l'excès le périmètre de cette surveillance**, sauf à remettre en cause l'équilibre entre les libertés fondamentales à protéger.

(2) L'article 1er du projet de loi dispose que « *le respect de la vie privée, notamment le secret des correspondances et l'inviolabilité du domicile, est garanti par la loi* » et qu'il ne peut y être porté atteinte « *que dans les seuls cas de nécessité d'intérêt public prévus par loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité* ». La Commission, particulièrement attachée au respect de ces principes généraux, souligne que **le droit à la protection des données à caractère personnel est un droit fondamental à part entière** qui mériterait, à ce titre, de figurer expressément dans la liste de ceux garantis par la loi dans le cadre des activités de renseignement. Elle souhaite également que soit réaffirmée, à côté du principe de proportionnalité, **la nécessaire subsidiarité de toutes les mesures de surveillance**, qui impose de limiter les atteintes aux libertés individuelles aux cas où le but poursuivi ne peut être atteint par un autre moyen moins intrusif.

(3) La Commission rappelle par ailleurs que **les activités de renseignement doivent être proportionnées à un nombre limité et précisément défini de finalités.** Or la Commission constate que l'**article 1er** du projet de loi ajoute aux cinq existantes **deux nouvelles finalités** – les intérêts essentiels de la politique étrangère et l'exécution des engagements européens et internationaux de la France et la prévention des violences collectives de nature à porter gravement atteinte à la paix publique – sans que soit précisément caractérisée chacune d'elle laissant ainsi une très large marge d'interprétation et autorisant potentiellement un recours très élargi aux activités et aux technologies du renseignement. S'agissant des « *intérêts essentiels de la politique étrangère* » et de « *l'exécution des engagements européens et internationaux de la France* », la Commission souhaite que les débats permettent une clarification de ces notions. Quant à la finalité de « *prévention des violences collectives de nature à porter gravement atteinte à la paix publique* », la Commission la juge trop floue et trop large et préconise sa suppression, l'objectif de prévention des violences collectives de nature à porter atteinte à la forme républicaine et à la stabilité des institutions étant par ailleurs couverte par la notion de « *sécurité nationale* ».

(4) Les **articles 1er à 3** du projet de loi redéfinissent le **régime juridique applicable aux techniques de recueil du renseignement** : modification des conditions d'utilisation des techniques actuelles (interceptions de sécurité ; accès administratif aux données de connexion),autorisation de recourir à de nouveaux dispositifs jusque-là réservés aux services de police judiciaire (captation, fixation, transmission et enregistrement de sons, d'images et de données informatiques ; géolocalisation en temps réel) et à des techniques nouvelles (sonde ; dispositif technique de proximité ou *IMSI-catcher* ; détection de « signaux faibles »).

D'une part, la Commission relève que ces articles **élargissent significativement le champ actuel des interceptions de sécurité et du recueil administratif des métadonnées.** Pour les interceptions de sécurité, ces articles suppriment leur caractère exceptionnel et étendent très largement ces interceptions non plus, comme actuellement, aux seules personnes ayant « un lien personnel et direct » avec une infraction présumée mais à l'ensemble des « *personnes appartenant à l'entourage de la personne visée* » lorsqu'elles « *sont susceptibles de jouer un rôle d'intermédiaire, volontaire ou non, pour le compte de celle-ci ou de fournir des informations* » sur l'une des finalités de l'interception.

Ces articles couplent automatiquement l'interception et le recueil des données de connexion de la personne (nouvel article L. 852-1 du code de la sécurité intérieure) et portent de 10 jours à un mois la durée de conservation des interceptions, augmentation qui avait été pourtant rejetée au cours des débats sur la loi renforçant les dispositions relatives à la lutte contre le terrorisme (II du nouvel article L. 822-2 du même code). La durée de conservation des données techniques de connexion recueillies par les services de renseignement est également augmentée, passant de trois à cinq ans (I du même article).

Ces dispositions ne soulèvent pas d'objection de principe de la part de la Commission, à condition que la notion d'« *entourage de la personne visée* » ne fasse pas l'objet d'une interprétation extensive.

D'autre part, la Commission s'est interrogée sur **l'extension prévue par le projet de loi des moyens des services de renseignement à de nouvelles techniques** prévues par les articles 2 et 3.

L'article 2 autorise, pour l'ensemble des finalités des activités de renseignement, la géolocalisation administrative en temps réel d'une personne, d'un véhicule ou d'un objet (nouvel article L. 851-6 du même code) et l'utilisation en cours d'opération, de dispositifs mobiles de proximité de captation directe de certaines métadonnées (dispositif dit *IMSI-catcher* ; nouvel article *L 851-7* du même code). Il permet également, pour les seuls besoins de la prévention du terrorisme, le recueil en temps réel, sur les réseaux des opérateurs de communications électroniques (sonde), des données de connexion de « *personnes préalablement identifiées comme présentant une menace* » (nouvel article L. 851-3 du même code), voire, à titre exceptionnel, l'utilisation du dispositif des *IMSI-catcher* pour intercepter directement le contenu des correspondances (nouvel article L. 851-7 du même code). Par ailleurs il permet également à des fins de prévention du terrorisme, l'exploitation, par les opérateurs de communications électroniques et les fournisseurs de services, des « *informations et documents traités par leurs réseaux* » (détection de « signaux faibles » par la pose de « boîtes noires » chez les opérateurs) afin de « *révéler, sur la seule base de traitements automatisés d'éléments anonymes, une menace terroriste* » (nouvel article L. 851-4 du même code). L'article 3 autorise, si aucun autre moyen légal n'est possible pour obtenir le même renseignement, le recours à des appareils de captation, de transmission et d'enregistrement de sons, d'images et de données informatiques (nouvel article L. 853-1 du même code) ainsi que l'introduction dans un véhicule, un lieu privé ou un système automatisé de traitement de données aux fins de poser, mettre en œuvre ou retirer de tels appareils (nouvel article L. 853-2 du même code).

Ces articles appellent plusieurs observations de la part de la Commission, qui recoupent les préoccupations déjà formulées par le Conseil national du numérique et la CNIL dans son avis sur le projet de loi.

S'agissant du recueil, en temps réel sur les réseaux des opérateurs, d'informations et documents relatifs à des personnes préalablement identifiées comme présentant une menace (article L. 851-3 dans sa rédaction proposée par le projet de loi), la Commission s'interroge sur le périmètre exact des données concernées au regard de la formulation retenue et souhaite qu'il soit précisé que seules les données de connexion puissent être recueillies.

La Commission est fortement préoccupée par l'usage préventif de sondes et d'algorithmes paramétrés pour recueillir largement et de façon automatisée des données anonymes afin de détecter une menace terroriste (« signaux faibles »).

La Commission estime que l'article L. 851-4, dans sa rédaction proposée par le projet de loi, ouvre la possibilité, à des fins de prévention du terrorisme, d'une collecte massive et d'un traitement généralisé de données. L'argument selon lequel cette surveillance porte initialement sur des données anonymes, traitées de façon automatique et algorithmique, ne saurait offrir de garanties suffisantes. Cet argument est d'ailleurs traditionnellement avancé à l'appui de la surveillance généralisée, qui a recours à des algorithmes qui lisent et exploitent des volumes massifs de données.

Par ailleurs, sur le plan juridique, les données concernées ne sont pas anonymes, puisque leur exploitation peut conduire, sous certaines conditions, à la levée de l'anonymat. Il s'agit donc d'un traitement de données à caractère personnel. La Commission s'interroge sur la conformité de la mesure proposée au regard des exigences posées par la CJUE, dans son arrêt *Digital Rights Ireland* du 8 avril 2014, qui rappelle que tout traitement de ce type doit être ciblé et proportionné.

Enfin, la Commission est particulièrement attentive à éviter des « effets de brèche » qui conduiraient à l'élargissement de ce dispositif à d'autres finalités que la prévention du terrorisme.

La Commission s'est interrogée sur la possibilité d'un encadrement strict de ce type de technologie de surveillance. En l'état des informations disponibles, cet encadrement ne lui est pas apparu envisageable. **C'est pourquoi la Commission appelle de ses vœux la suppression de l'article L 851-4 du projet de loi.**

La Commission regrette que les **dispositifs administratifs de localisation en temps réel** d'une personne, d'un véhicule ou d'un objet **et de captation, de transmission et d'enregistrement de sons, d'images et de données informatiques** ne soient **pas assortis de garanties équivalentes à celles prévues, pour les professions protégées, par le code de procédure pénale lorsqu'ils sont mis en œuvre dans un cadre judiciaire.** À cet égard, devraient être exclus de la géolocalisation administrative, au même titre que la géolocalisation judiciaire, les lieux mentionnés aux articles 56-1 à 56-4 (cabinet et domicile d'un avocat, locaux de presse, cabinet d'un médecin, notaire ou huissier, etc.) et le bureau ou le domicile des personnes mentionnées à l'article 100-7 du code de procédure pénale (député, sénateur, magistrat, etc.).Elle souhaite par ailleurs qu'il soit précisé que la géolocalisation en temps réel est effectuée par « *un agent individuellement désigné et dûment habilité* » comme c'est le cas pour les autres techniques de recueil du renseignement.

Ces articles **ne définissent pas non plus avec suffisamment de précision les conditions dans lesquelles des dispositifs aussi intrusifs pour la vie privée peuvent être utilisés**, s'agissant notamment des « *personnes préalablement identifiées comme présentant une menace* » dont les métadonnées ou les correspondances peuvent être saisies en temps réel et du champ de la captation, de la transmission et de l'enregistrement des « *données informatiques transitant par un système automatisé de données ou contenues dans un tel système* ».

Quoique soumise à des garanties renforcées (limitation des finalités, principe de subsidiarité, renforcement de la motivation de la demande, durée d'autorisation limitée à respectivement deux mois et 30 jours pour les mesures autorisées par l'article 3), l'utilisation de ces dispositifs est susceptible de conduire à une **surveillance indiscriminée des personnes** et à une **collecte indifférenciée des données,** sans que soient apportées de surcroît toutes les garanties d'un contrôle strict de leur mise en œuvre. Ainsi le recours aux *IMSI-catcher* permet par exemple la collecte de données à caractère personnel d'un nombre indéterminé de personnes situées dans l'environnement géographique de celle visée par la mesure.

L'article 3 crée également un cadre spécifique aux **interceptions de communications électroniques émises ou reçues à l'étranger.** La Commission relève tout d'abord que le cadre applicable à la surveillance internationale est, en l'état, très flou : en particulier, aucune indication sur les techniques précisément utilisées n'est fournie. Par ailleurs, compte tenu du caractère mondial des réseaux numériques, l'essentiel des communications des citoyens français est émis ou reçu à l'étranger, notamment aux États-Unis où sont domiciliés de nombreux serveurs. Il y a donc un risque que cette surveillance internationale, beaucoup moins encadrée, s'applique indirectement aux citoyens français. C'est pourquoi la Commission appelle de ses vœux une clarification du champ de cette surveillance internationale et de son régime. Elle préconise notamment que l'exigence de recourir à un « *agent individuellement désigné et dûment habilité* » prévue pour d'autres techniques de renseignement soit étendue à ce type de surveillance.

(5) Le projet de loi soumet au contrôle d'une **nouvelle autorité administrative indépendante** – la Commission nationale de contrôle des techniques de renseignement (CNCTR) – et au **juge administratif** – une formation spécialisée du Conseil d'État statuant en premier et dernier ressort – l'ensemble des techniques de recueil du renseignement (accès administratifs aux données de connexion, interceptions de sécurité, localisation, sonorisation de certains lieux et véhicules, captation d'images et de données informatiques), à l'exception des mesures de surveillance internationale.

La création de cette nouvelle autorité administrative, qui remplacera la Commission nationale de contrôle des interceptions de sécurité chargée de formuler un avis sur les demandes d'interception de sécurité, et la personnalité qualifiée qui se prononce sur les demandes d'accès aux métadonnées, unifie le contrôle

des techniques de renseignement. Les précisions apportées quant à sa composition (conditions de nomination, règles de déontologie et d'incompatibilité) constituent d'importantes garanties d'indépendance et d'impartialité. Le spectre large des missions qui lui sont dévolues (avis préalable, pouvoir de recommandation tendant à interrompre la mise en œuvre d'une technique, pouvoir de saisine du Conseil d'État, etc.) renforce la portée du contrôle qu'elle exerce sur ces activités.

Toutefois, la Commission considère que l'autorité et l'efficacité du contrôle de la CNCTR devront être consolidées en veillant à la doter des **moyens budgétaires et humains nécessaires à l'exercice de l'ensemble de ses missions et à garantir son indépendance dans le mode de désignation de ses membres comme de ses services.** Il appartiendra au Gouvernement, au cours des débats, de préciser les budgets et les compétences humaines dont il entend doter cette autorité.

La Commission souhaite également que toutes les précisions nécessaires soient apportées à l'article 1er du projet de loi afin de lui donner les moyens juridiques de procéder, à tout moment de la mise en œuvre de la technique de recueil du renseignement, à tous les **contrôles, sur pièce et sur place**, utiles. La Commission insiste sur la nécessité pour la CNCTR de pouvoir mener des contrôles actifs, *a priori* comme *a posteriori*, sur les différentes technologies utilisées, leur champ d'application ou leurs conditions de mise en œuvre.

L'article 1er prévoit que, pour l'accomplissement de sa mission, la CNCTR « *dispose d'un droit d'accès aux autorisations, relevés, registres, données collectées, transcriptions et extractions* » (nouvel article L. 833-2 du code de la sécurité intérieure). La Commission estime que la CNCTR devrait être systématiquement destinataire de ces éléments afin d'exercer pleinement ses missions.

Elle partage les préoccupations du Conseil national du numérique qui estime crucial de doter la CNCTR de pouvoirs d'enquête suffisants et regrette que cette dernière soit simplement informée de l'autorisation donnée par le Premier Ministre de procéder à une géolocalisation ou à la mise en place d'un « dispositif de proximité » pour appréhender des données de connexion en cas « d'urgence absolue ».

En outre, la Commission recommande la désignation, au sein de la CNCTR, d'une personnalité qualifiée pour sa connaissance en matière de droit de la protection de la vie privée et des données à caractère personnel, nommée sur proposition du président de la CNIL.

Enfin, la Commission estime que toute technique de surveillance et ses évolutions, présentant une menace particulière pour les libertés individuelles, devraient être soumises à l'autorisation préalable de la CNCTR qui devrait en encadrer les conditions d'utilisation techniques.

(6) La Commission regrette qu'aucune disposition ne vienne renforcer la sanction pénale des infractions résultant d'actions illégales, contrepartie pourtant nécessaire d'une loi sur le renseignement et déplore les possibilités de recours limitées et en pratique difficiles à mettre en œuvre offertes aux citoyens pour contester les mesures de surveillance exercées à leur encontre.

Par ailleurs, lorsque le Premier ministre ne donne pas suite à ses recommandations, il est prévu que la CNCTR puisse saisir le Conseil d'État à la majorité absolue de ses membres (nouvel article L. 821-6 du code de la sécurité intérieure). Une saisine à la demande de deux membres est toutefois possible en cas de recours à des techniques particulièrement intrusives (nouvel article L. 853-2 du même code). La Commission préconise de généraliser cette possibilité quelle que soit la technique de recueil du renseignement utilisée.

(7) La Commission appelle enfin l'attention du législateur sur l'absence de disposition spécifique relative au **signalement des activités illégales de surveillance administrative**, l'article 1er du projet de loi se bornant à prévoir que la CNCTR peut s'autosaisir ou être saisie par « *toute personne y ayant un intérêt direct et personnel* ». La loi du 6 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière a certes interdit toute mesure défavorable prise à l'encontre d'une personne qui, de bonne foi, témoigne sur des faits constitutifs d'un crime ou d'un délit. Mais cette disposition ne couvre pas le signalement d'activités qui, sans être *stricto sensu* pénalement répréhensibles, relèveraient de manquements à la morale, à l'éthique ou à l'intérêt général. Dès lors, le Parlement pourrait débattre de l'opportunité d'instaurer un canal d'information sécurisé pour les agents des services de renseignement, par la création d'un statut protecteur des lanceurs d'alerte dans le domaine sensible des activités de surveillance administrative ou par l'aménagement de dispositifs administratifs internes à chaque service concerné.

[1] *CEDH, 24 avril 1990, Kruslin c. France.*

[2] *Voir CJUE, 13 mai 2014,* Google Spain c. AEPD. *La protection des données à caractère personnel figure par exemple, en tant que tel, à l'article 8 de la Charte des droits fondamentaux de l'Union européenne.*

[3] *L'article L. 241-2 du code de la sécurité intérieure mentionne la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France ainsi que la prévention du terrorisme, de la criminalité organisée et de la reconstitution ou du maintien de groupements dissous.*

[4] *Qui figure actuellement à l'article L. 241-2 du code de la sécurité intérieure.*

[5] *Communiqué de presse du Conseil national du numérique du 19 mars 2015.*