Sommaire

Avant-propos

Au cours de l'année 2012-2013, la Commission nationale de contrôle des interceptions de sécurité (CNCIS) est entrée dans une période de transition, marquée par le vote de plusieurs textes législatifs.

Ainsi, l'ordonnance du 12 mars 2012 relative à la partie législative du Code de la sécurité intérieure a conduit à l'abrogation, depuis le 1er mai 2012, de la loi du 10 juillet 1991 et à l'intégration à droit constant de ses dispositions administratives dans le Code de la sécurité intérieure. Cette ordonnance n'a pas, à ce jour, été ratifiée par le Parlement.

De plus, la loi du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme a prorogé pour trois ans le dispositif expérimental de recueil de données techniques de communications instauré par la loi du 23 janvier 2006.

Pour autant, ces deux textes ne répondent pas aux attentes réformatrices portées par la CNCIS. Comme je l'ai souligné lors des auditions dont j'ai fait l'objet l'an passé devant les assemblées parlementaires : il est désormais indispensable et urgent de réviser les dispositions issues de la loi du 10 juillet 1991 qui ne sont plus en parfaite adéquation avec les exigences imposées par les évolutions majeures de la technologie au cours des vingt dernières années.

Les modifications nécessaires, qui devront comporter un accroissement des compétences et moyens de l'autorité administrative indépendante (AAI), sont incontestablement nombreuses. Celles qui doivent intervenir le plus rapidement sont l'inscription dans la loi de la pratique de l'avis *a priori* de la Commission pour toute demande d'interception de sécurité comme de géolocalisation en temps réel, et l'unification des cadres légaux de recueil de données techniques de communications sous l'autorité du Premier ministre.

Cet appel de la CNCIS à l'actualisation des textes législatifs dans le domaine du renseignement technique, réitéré sans relâche depuis plusieurs années, a rencontré un écho important dans les récents travaux consacrés à l'avenir du renseignement. Ainsi, le Livre blanc sur la défense et la sécurité nationale rendu public le 29 avril 2013, le rapport de la mission parlementaire sur l'évaluation du cadre juridique applicable aux services de renseignement déposé le 14 mai 2013 et le rapport de la commission d'enquête sur le fonctionnement des services de

renseignement français dans le suivi et la surveillance des mouvements radicaux armés déposé le 24 mai 2013 ont tous mis l'accent sur la nécessité de moderniser et renforcer le cadre légal dans lequel doit s'exercer l'action des services de renseignement.

Les auteurs du rapport parlementaire du 14 mai 2013 vont même plus loin lorsqu'ils préconisent que la CNCIS serve de base à la création d'une AAI qui aurait des compétences élargies : cette Commission s'assurerait du respect des principes de légalité et de proportionnalité dans l'usage par les services de renseignement des moyens techniques de collecte d'informations.

Toutefois, je tiens à préciser qu'une telle structure ne pourra remplir ses missions avec succès que si elle bénéficie de ce qui garantit à la CNCIS, depuis 1991, autorité et efficacité dans la protection des libertés : la présence en son sein d'une part de membres parlementaires issus de manière paritaire de la majorité et de l'opposition, d'autre part de magistrats de l'ordre judiciaire, en qualité de membres et d'agents.

C'est en ce sens qu'elle peut, comme le constatent les auteurs du rapport du 14 mai 2013, être qualifiée de « modèle abouti ». Je souhaite donc pour ma part que ces propositions parlementaires débouchent sur un accroissement du champ de compétence de la CNCIS vers d'autres techniques spéciales d'enquête telles que l'infiltration, la sonorisation, la captation d'images ou de données informatiques, dont l'usage n'est pour l'instant, en matière administrative, pas prévu par les textes.

La loi relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale ne sera vraisemblablement pas, en l'état du texte en cours d'examen au Parlement, celle du renforcement dont l'encadrement légal des services de renseignement a tant besoin. Je le regrette, tout comme je déplore de n'avoir à aucun moment été officiellement consulté lors de l'élaboration de ce projet de loi, qui, pourtant, cite les travaux de la CNCIS dans son exposé des motifs.

Quel que soit le vecteur législatif qui sera finalement retenu, il est impératif qu'il soit adopté rapidement et qu'il constitue l'occasion d'un vrai débat pour une réforme à la hauteur des enjeux. Il est tout aussi essentiel que la CNCIS soit associée dès les travaux préparatoires et durant l'ensemble du processus normatif, conformément aux dispositions qui prévoient la consultation des AAI sur les projets portant sur leur domaine de compétence.

Forte de son expertise unique, issue des contrôles effectués comme des avis rendus depuis plus de vingt ans, l'institution que je préside prendra, comme à chaque fois qu'un projet de texte lui a été soumis depuis 1991, toute sa part dans les travaux d'élaboration de cette législation d'avenir.

Je ne doute pas que la parole de la CNCIS, que je porte en compagnie des deux membres parlementaires qui la composent, M. Jean-Jacques HYEST, sénateur de la Seine-et-Marne et M. Jean-Jacques URVOAS, député du Finistère, l'un et l'autre très investis dans leur mandat au sein de la Commission, sera entendue.

Enfin, j'adresse mes plus vifs remerciements à M. Bertrand WARUSFEL, professeur à l'université de Lille 2, et à Mme Virginie PELTIER, maître de conférences à l'université Montesquieu à Bordeaux, pour leur contribution à ce 21e rapport d'activité.

Hervé PELLETIER
Président de la Commission

« CONTRÔLER LES SERVICES » : ODE À LA COMMISSION NATIONALE DE CONTRÔLE DES INTERCEPTIONS DE SÉCURITÉ

Jean-Jacques URVOAS
Député du Finistère,
président de la Commission des lois
de l'Assemblée nationale

Dans notre pays, la raison d'État a toujours reculé au profit du droit sous la pression des événements. C'est ainsi que la Commission nationale de contrôle des interceptions de sécurité (CNCIS), bien que fruit d'un accident de l'histoire, a fini par s'imposer comme une référence en raison de son précieux apport à un fonctionnement vertueux de notre démocratie.

Autorité administrative indépendante, elle intervient au cœur du réacteur étatique et, sans mettre à mal notre dispositif de sécurité, assure à nos concitoyens l'exercice paisible de leurs libertés individuelles.

Toutefois, la large acceptation dont elle jouit désormais ne saurait occulter les intenses débats juridiques qui ont précédé sa création. D'autant que, confronté à des besoins similaires à ceux constatés en 1991, le législateur connaît aujourd'hui des questionnements identiques.

Les interprétations de l'article 66 de la Constitution en matière d'écoutes administratives : autorité judiciaire ou tierce ?

Comme le rappelle Louis Favoreu, le Titre VIII de la Constitution consacré à l'autorité judiciaire a longtemps été délaissé par la doctrine[1]. En particulier, l'article 66 était considéré comme une déclaration de principe dénuée de toute substance, un ajout symbolique défendu par le professeur Marcel Waline lors de la rédaction de notre loi fondamentale. René Chapus s'étonnait même de cette prévention à l'égard de la juridiction administrative qui, à ses yeux, « a cessé de pouvoir être suspectée de ne pas assurer une protection normale des droits et libertés des administrés[2] ».

Néanmoins, dans le même temps, plusieurs décisions du Conseil constitutionnel réaffirmaient avec force le statut de gardienne des libertés individuelles conféré à l'autorité judiciaire. En témoignent notamment[3] les décisions n°76-75 du 12 janvier 1977 concernant la fouille des véhicules, n° 83-164 DC du 29 décembre 1983 et n° 84-184 DC du 29 décembre 1984 concernant les perquisitions par l'administration fiscale, ou encore n° 84-181 DC du 11 octobre 1984 concernant les visites d'entreprises de presse ordonnées par la Commission pour la transparence et le pluralisme[4].

En outre, le juge constitutionnel ne distinguait pas de manière rigide les activités de police judiciaire et administrative, au profit des officiers de police judiciaire. En effet, le Conseil reconnaissait au législateur la faculté de confier à ces derniers « des missions de prévention des atteintes à l'ordre public qui ressortissent normalement à la police administrative[5] » sans que le principe de séparation des pouvoirs n'en souffrît pour autant.

Or, dans les années 1980, la question des écoutes téléphoniques offrit une nouvelle occasion de réaffirmer cette prérogative de l'autorité judiciaire. La Cour de cassation établit ainsi pour la première fois un lien entre cet enjeu et l'article 66 dans un arrêt de l'assemblée plénière en date du 24 novembre 1989 (« affaire Baribeau »)[6]. Il est vrai que la thématique

---

1) Louis Favoreu *in* « La Cour de cassation, le Conseil constitutionnel et l'article 66 de la Constitution », *Recueil Dalloz,* 1986, chronique, p. 172.
2) Cité *in* Louis Favoreu, *ibid.*
3) Pour une énumération exhaustive, se reporter à Louis Favoreu, *ibid.*, p. 173.
4) Cette dernière décision présente un intérêt particulier dans le cadre de la présente réflexion puisque la commission en question relevait de la catégorie des autorités administratives indépendantes.
5) Décision n° 80-127 DC du 20 janvier 1981.
6) Voir à ce sujet Pierre Kayser et Thierry Renoux, « La Cour de cassation et l'article 66 de la Constitution : à propos de l'arrêt de l'assemblée plénière du 24 novembre 1989 sur les écoutes téléphoniques », *Revue française de droit constitutionnel*, 1990, n°1, p. 141.

des interceptions agitait alors l'Europe occidentale après la condamnation par la Cour européenne des droits de l'homme (CEDH) de plusieurs de nos voisins (le Royaume-Uni notamment) puis de la France elle-même par les arrêts *Huvig* et Kruslin, en avril 1990. Pareille sanction s'inscrivait d'ailleurs en cohérence avec les décisions judiciaires précédemment rendues dans notre pays sur ces dossiers. Partant, l'arrêt précité de la Cour de cassation exhortait le législateur à adopter une législation afin de se mettre en conformité avec l'article 8 de la CEDH (infléchissant de la sorte sa position antérieure, comme Jean Pradel l'a souligné [1]).

Néanmoins, aucun contentieux n'avait émergé autour de la question des écoutes administratives, pourtant soumises aux mêmes carences législatives. Si bien que les interprétations de l'article 66 pouvaient être soit étendues à ce champ (au motif que l'intrusion est identique en police judiciaire et administrative), soit considérées comme non pertinentes en ce domaine (au plan doctrinal).

Sur ce point, le rapport de la Commission d'étude sur les écoutes téléphoniques, remis à Pierre Mauroy le 25 juin 1982 par Robert Schmelck, proposa une réponse tout à la fois tempérée et originale à la question des autorités susceptibles d'autoriser une interception. Il signalait ainsi que « même si l'intervention du juge peut se recommander du rôle imparti à l'autorité judiciaire en matière de liberté individuelle par l'article 66 de la Constitution, il reste que cet article laisse au législateur une marge d'appréciation puisque l'autorité judiciaire doit intervenir "dans les conditions définies par la loi".» Fondamentalement hétérodoxe, pareille exégèse constitutionnelle s'appuyait sur la jurisprudence de la CEDH qui ouvrait la possibilité d'un contrôle *ex post* confié à une autorité non judiciaire pourvu qu'elle jouît des nécessaires garanties d'indépendance.

Dans cette optique, le rapport Schmelck suggérait la création d'une AAI chargée non d'autoriser les interceptions mais de les contrôler, et composée de quatre parlementaires, d'un conseiller d'État, de deux membres de la Cour de cassation et de deux personnalités qualifiées. La nature autant que la composition de l'instance préconisée démontraient la prise de distance opérée avec une interprétation rigide de l'article 66. Aujourd'hui encore, cette « audace » mérite d'être soulignée en ce qu'elle répondait sans doute à la ferme volonté de maintenir les juges en dehors du périmètre des écoutes administratives (*cf. infra*).

Dans une perspective moins utilitariste et beaucoup plus doctrinale, le Conseil d'État, lorsqu'il fut saisi pour avis en mai 1991 sur le projet de loi relatif à l'interception des correspondances émises par la voie des télécommunications, entérina ce même raisonnement. Dans son rapport public de 1991, il estimait en effet « que les dispositions de l'article 66

1) Jean Pradel, « Écoutes téléphoniques et Convention européenne des droits de l'homme », *Recueil Dalloz*, 1990, p. 15-20.

de la Constitution selon lesquelles l'autorité judiciaire est garante de la liberté individuelle n'obligent pas à placer sous le contrôle de cette autorité les interceptions de sécurité qui constituent des mesures de police administrative ne portant pas atteinte à la liberté individuelle au sens de cet article[1] ».

Ce faisant, la juridiction interprétait l'article 66 comme un *habeas corpus* portant non sur l'ensemble des libertés individuelles mais sur la seule liberté de ne pas être détenu arbitrairement. Dans le même esprit, par le biais de la décision n°99-416 DC du 23 juillet 1999, le Conseil constitutionnel opéra un revirement jurisprudentiel en adoptant cette même position, cessant dès lors de rattacher la protection de la vie privée à l'article 66 de la Constitution pour la faire découler de l'article 2 de la Déclaration des droits de l'homme et du citoyen. Par la suite, il consolida encore cette exégèse dans sa décision n°2005-532 DC du 19 janvier 2006 concernant une loi antiterroriste qui portait notamment des dispositions relatives aux interceptions de sécurité[2].

De surcroît, le juge constitutionnel a établi une distinction entre la police judiciaire, dédiée à la répression d'une infraction ainsi qu'à la recherche de ses auteurs, et la police administrative qui a pour but de « faire cesser un trouble déjà né, fût-il constitutif d'infraction, et [de concourir à] la prévention des infractions ». Dans ces conditions, si les moyens octroyés à la première sont soumis à l'autorisation du juge (la jurisprudence est constante sur ce point), ceux dévolus à la seconde relèvent de la responsabilité du pouvoir exécutif[3].

En définitive, dans sa décision de janvier 2006, le Conseil constitutionnel a considéré que la loi de 1991 relative aux interceptions de sécurité fournissait un utile modèle pour fonder une réflexion spécifique à cet enjeu. L'évolution jurisprudentielle et doctrinale a donc consacré le recours à une AAI pour répondre aux naturelles exigences démocratiques, notamment portées par la CEDH, en matière de contrôle des interceptions de sécurité administratives.

Les atouts des AAI pour le contrôle de l'État secret

La controverse doctrinale dont nous avons rendu compte est susceptible de surprendre bien des Français, tant elle reflète une farouche

---

1) Conseil d'État, *Rapport public 1991*, Paris, La Documentation française, 1992, p. 62.
2) *Cf.* en particulier le « Commentaire de la décision n°2005-532 DC du 19 janvier 2006 »*, in Les cahiers du Conseil constitutionnel*, n°20, 16 p.
3) Décision n°2005-532 DC du 19 janvier 2006. Jurisprudence désormais consolidée par la décision n° 2011-625 DC du 10 mars 2011.

opposition à toute introduction de juges dans le processus d'autorisation ou de contrôle des écoutes administratives. Le rapport Schmelck repoussait d'ailleurs une telle évolution au motif qu'elle induirait un « transfert de responsabilité » du pouvoir exécutif au pouvoir judiciaire dans un domaine si éminemment régalien[1]. Peu de pays ont d'ailleurs opté pour cette solution (à l'image de l'Espagne et, dans une moindre mesure, de la Norvège). Car, indépendamment des questions constitutionnelles, tous les services de renseignement se montrent résolument rétifs à l'intrusion dans leur périmètre d'intervention, où bien entendu s'impose un absolu secret, de magistrats dont l'activité obéit au contraire à des impératifs incontournables de transparence et de publicité des débats.

Encouragés par le caractère libéral de la jurisprudence de la CEDH, les gouvernements ont donc recherché des solutions médianes : l'Allemagne ou la Belgique ont opté pour une commission administrative dépendant du Parlement[2], tandis que le Royaume-Uni s'en remet à un haut fonctionnaire (le *commissionner*) qui agit en toute indépendance et peut saisir un tribunal spécial en tant que de besoin. La France, quant à elle, a eu recours à des AAI, structures originales d'inspiration étrangère (allemande, étatsunienne, canadienne ou suédoise avec l'exemple de *l'ombudsman*) introduites par la loi qui créa la Commission nationale de l'informatique et des libertés (CNIL) en 1978.

C'est sans doute Jean-Pierre Chevènement qui a le mieux cerné les raisons du succès rencontré par les AAI lors d'une séance publique à l'Assemblée nationale, le 4 juin 1998 : « Voilà une vingtaine d'années que le paysage administratif français s'est enrichi de ces instances, dépourvues de la personnalité morale, mais s'inscrivant en dehors de la hiérarchie des administrations centrales et de leurs chefs que sont les ministres. L'objectif est clair : les pouvoirs publics attendent de ces institutions qu'elles s'acquittent de leur tâche comme le feraient les magistrats, c'est-à-dire avec impartialité, objectivité et indépendance. L'accroissement du nombre de ces instances est peut-être la preuve de leur succès ».

De fait, comme le rappelle le Conseil d'État, les AAI font partie de la sphère administrative française et, à ce titre, ont la faculté d'« agir au nom de l'État sans [toutefois] être subordonnées au Gouvernement[3] ». Pareille indépendance tient tout à la fois à la collégialité et la composition de ces instances (parlementaires, hauts fonctionnaires…), à l'irrévocabilité du

1) Il soulignait en outre l'urgence parfois nécessaire en matière d'autorisation – argument qui, en l'espèce, nous semble beaucoup moins pertinent que le premier. Rappelons que la commission Marcilhacy-Monory, dans son rapport de 1973 consacré aux interceptions de sécurité, avait proposé que l'autorisation et le contrôle fussent réalisés par un juge de la Cour de cassation secondé par deux autres magistrats.
2) La « commission G10 » en Allemagne, la « commission BIM » en Belgique.
3) *In* Conseil d'État, *Rapport public 2001. Jurisprudence et avis de 2000. Les autorités administratives indépendantes*, Paris, La Documentation française, 2001, p. 257.

mandat de leurs membres, voire à l'impossibilité pour le Gouvernement d'opposer un veto aux décisions prises[1].

L'ensemble de ces critères participent donc à la recherche d'une absolue impartialité en même temps que leur usage témoigne d'une certaine méfiance tant à l'égard du pouvoir politique qu'administratif ou même judiciaire – l'un des objectifs étant d'éviter de recourir à des magistrats (Jean-Pierre Chevènement le suggère en creux en employant une comparaison au conditionnel : « Comme le feraient les magistrats »). Dans cette logique, les premières AAI furent dédiées à la protection des libertés fondamentales, à l'instar de la CNIL ou de la Commission d'accès aux documents administratifs (CADA). Fort laudateur à leur sujet, René Rémond y voyait « autant de dispositions qui concourent à faire régresser l'empire du secret et à contrarier l'arbitraire[2] ». Après l'alternance de 1981, elles furent utilisées dans le domaine de la presse et de l'audiovisuel à cette même fin, que reconnaîtra le Conseil constitutionnel en qualifiant la Haute Autorité de la communication audiovisuelle de « garantie fondamentale pour l'exercice d'une liberté publique[3] ».

Aujourd'hui très sollicitées en matière de régulation économique[4], elles n'en continuent pas moins d'incarner une solution adaptée aux enjeux liés au respect des libertés fondamentales (citons par exemple, au-delà de la création de la CNCIS en 1991, celle de la Commission consultative du secret de la défense nationale (CCSDN) en 1998, du Contrôleur général des lieux de privation de liberté en 2007 ou du Défenseur des droits en 2011…).

En matière d'écoutes téléphoniques, sous la pression conjointe de condamnations de la France par la CEDH, de l'arrêt précité de la Cour de cassation ou de faits divers (affaire du pasteur Doucé…), le gouvernement de Michel Rocard décida de mettre en application les préconisations du rapport Schmelck, qui n'avait jamais été rendu public. Il se rangea donc à l'idée d'instituer une autorité administrative dénommée Commission nationale de contrôle des interceptions de sécurité. Le rapport Schmelck justifiait ainsi ce choix (après avoir écarté l'option du juge judiciaire pour les raisons précédemment évoquées) : « Dans le domaine des écoutes téléphoniques, qui est politiquement très délicat et où les abus potentiels sont considérables, l'existence d'une instance indépendante, exerçant *a posteriori* un contrôle sur l'action des autorités responsables paraît de

1) Éléments évoqués dans le rapport précité, p. 291-3. Le dernier point paraît sujet à caution, notamment pour ce qui concerne la CNCIS.
2) *In* René Rémond, *Histoire de France, tome 6 : Le siècle dernier (1918-2002)*, Paris, Fayard, 2003, p. 779.
3) Décision nº 84-173 DC du 26 juillet 1984.
4) Le Conseil d'État (*in Rapport public 2001…*, *op. cit.*, p. 267) estime qu'il s'agit d'un domaine privilégié d'intervention des AAI.

nature à concilier les exigences de l'intérêt public et la garantie des droits et libertés des individus[1] ».

Là où le rapport Schmelck préconisait la désignation de quatre parlementaires, d'un membre du Conseil d'État, de deux membres de la Cour de cassation et de deux personnalités qualifiées, le texte voté opta pour la nomination d'un haut fonctionnaire issu du Conseil d'État ou de la Cour de cassation accompagné de deux parlementaires. Mais, hormis ces détails techniques, la recherche de « personnalités indépendantes du pouvoir exécutif […] afin d'assurer à l'organe de contrôle une autorité morale indiscutable[2] » est patente. D'une manière générale, le modèle de la CNIL a constitué une indéniable source d'inspiration pour la conception et la création de cette nouvelle instance[3].

L'avènement de la CNCIS constitua donc une nouveauté dans le paysage du contrôle des décisions de l'État en matière d'interceptions de sécurité puisque, auparavant, la décision du Premier ministre du 28 mars 1960 créant le Groupement interministériel de contrôle (GIC) avait institué une commission composée d'un représentant des ministères de l'Intérieur ainsi que des Armées et présidée par un représentant du chef du Gouvernement. Cette commission était chargée d'examiner la conformité de la production du GIC avec les besoins des services et celle des demandes formulées par ces derniers avec la réalité de leurs missions. En cas de difficulté, elle pouvait solliciter une réunion en comité interministériel.

Toutefois, avec la CNCIS comme avec sa devancière, l'autorisation de l'écoute procède uniquement du pouvoir exécutif, les seules fonctions d'avis et de contrôle ayant été « externalisées » au profit de l'AAI créée en 1991. En outre, le Conseil d'État saisi pour avis n'a pas admis qu'il soit octroyé à cette dernière le pouvoir d'ordonner au Premier ministre d'interrompre une interception de sécurité considérée comme illégale au motif que l'article 20 de la Constitution confie l'administration au Gouvernement[4]. Les prérogatives de l'instance ont donc clairement été bornées, un partage des tâches établi qui concilie l'efficacité et les impératifs démocratiques.

Néanmoins, en dépit de la limite ainsi instituée, la CNCIS a bénéficié dès son entrée en fonction de la bienveillance du Premier ministre qui a accepté que le contrôle *a posteriori* prévu par la loi se mue en avis de mise en œuvre *ex ante.* Cette pratique a été officiellement confirmée par une directive du chef du gouvernement en date du 18 février 2008,

---

1) Reproduit *in* Commission nationale de contrôle des interceptions de sécurité, *Premier rapport d'activité, 1991-1992*, Paris, La Documentation française, 1993, p. 108.
2) *Ibid.*
3) *Ibid.*, p. 131 ainsi qu'entretien avec Bruno Genevois, rapporteur de la commission Schmelck.
4) Conseil d'État, *Rapport public 1991*, *op. cit.*, p. 62.

dans laquelle elle est présentée comme « la mieux à même de répondre à l'objectif de protection efficace des libertés poursuivi par le législateur ». Grâce à une coutume bien établie, la CNCIS a donc acquis une aura particulière qui respecte scrupuleusement la lettre constitutionnelle et la jurisprudence de la CEDH.

* * *

La CNCIS représente indubitablement une instance tout à fait spécifique au sein du paysage administratif français en ce qu'elle intervient au cœur du pouvoir régalien afin de s'assurer que des pratiques spéciales d'investigation sont mises en œuvre en conformité avec la loi. Exemple unique, sa création n'a pu survenir qu'à la suite d'évolutions doctrinales majeures qui ont consacré le recours à une autorité administrative indépendante comme la solution la plus adaptée au double défi constitué par le respect de l'État de droit et les exigences inhérentes au pouvoir exécutif. En ce sens, elle a contribué à dessiner un modèle, une véritable source d'inspiration pour le législateur qui doit faire face à des problématiques similaires.

En effet, si la France a été contrainte en 1991 de combler les lacunes de son droit, force est de constater que les évolutions technologiques et les mutations de la menace contre la sécurité intérieure ou extérieure laissent aujourd'hui les services de renseignement quelque peu démunis. L'heure semble donc venue de remédier à de nouvelles carences de notre droit, de doter les administrations du renseignement de nouveaux moyens d'action tout en répondant à des critères exigeants en matière de contrôle de légalité et de proportionnalité. Or, la simple mise en place de la CNCIS a tranché nombre de controverses juridiques et permet d'envisager une réponse équilibrée et satisfaisant à la double exigence précitée. Au surplus, vingt années d'exercice ont démontré la pertinence de la structure et des règles qui la régissent. En ce domaine, la révolution peut résider dans l'imitation.

Pour un approfondissement du cadre juridique des interceptions de sécurité

Bertrand WARUSFEL
Professeur à l'université Lille 2,
avocat au barreau de Paris

La CNCIS a fêté récemment les vingt ans de la loi du 10 juillet 1991 et de son institution en tant qu'AAI. Une fois passé ces moments de célébration, viennent ceux de ce que l'on me permettra d'appeler la rétro-prospective, c'est-à-dire l'analyse de l'expérience acquise en vue de préparer l'avenir.

La Commission l'a elle-même souhaité dès l'an dernier en écrivant dans son précédent rapport qu'elle formait le vœu « que le débat soit désormais ouvert sur une réforme de la loi n° 91-546 du 10 juillet 1991, au regard des évolutions technologiques en matière de communications électroniques et des nouvelles formes de menaces qui emportent des conséquences importantes dans l'équilibre entre, d'une part les enjeux de protection du secret des correspondances et de la vie privées, et, d'autre part les exigences de sécurité » (CNCIS, rapport 2011-2012, p. 39). Cette brève contribution s'inscrit dans ce cadre.

S'agissant de la question toujours sensible des interceptions de sécurité, comme l'actualité internationale récente et le scandale *Prism* nous le rappellent clairement, il me semble que l'avenir doit être marqué par une double exigence : suivre efficacement l'évolution rapide des techniques de communication tout en consolidant l'État de droit, et ce dans le contexte plus large de la mise en place d'un véritable droit de la sécurité nationale.

Suivre l'évolution rapide des techniques de communication

Le début du XXIe siècle est indiscutablement marqué par une intensification et une diversification de l'usage des outils numériques de communication et de traitement de l'information. Issu de la fusion

technologique entre l'informatique et les télécommunications, le nouveau domaine des « communications électroniques » – bien qu'assez mal dénommé (puisque c'est en réalité son caractère numérique qui est central et non le fait que les traitements numériques s'effectuent principalement grâce à des moyens électroniques) – a vocation à unifier les usages et les problématiques de traitement et de transmission de l'information, quel que soit l'outil utilisé (ordinateur fixe ou portable, tablette, téléphone mobile, mais aussi tous les systèmes professionnels ou domestiques qui « embarquent » des moyens de traitement et de transmission).

Dès lors que les modes de communication se multiplient et se complètent, le besoin de la puissance publique de pouvoir – dans des cas limitativement prévus et touchant la sécurité nationale – en assurer l'interception, doit également suivre cette évolution. D'où surgit une première interrogation relative à la définition légale du périmètre des communications pouvant faire l'objet d'interceptions de sécurité.

La loi de 1991 a retenu la formule concise des « correspondances émises par la voie des communications électroniques » (aujourd'hui reprise par les articles L. 241-1 et suivants du Code de la sécurité intérieure). Si le renvoi à la notion de « communications électroniques » définie par le Code des postes et des communications électroniques paraît s'imposer (puisque ce sont bien les opérateurs des réseaux de communication électronique, régis par le code du même nom, qui se voient chargés de permettre la réalisation des interceptions sur leurs réseaux), on peut cependant se demander s'il ne serait pas préférable d'harmoniser le texte avec celui du Code pénal (issu de la même loi de 1991) qui sanctionne la violation des « correspondances émises, transmises ou reçues par la voie électronique » (article L. 226-15, 2e alinéa). Cette dernière formulation a en effet l'avantage d'être plus proche de celle donnée par l'article 3 de la convention de Budapest sur la cybercriminalité du 23 novembre 2001 qui vise l'interception « effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique ».

Plus délicate est l'identification des différentes formes de communications électroniques qui doivent être considérées comme des correspondances au sens de l'article L. 241-1 du Code de la sécurité intérieure. Certaines formes en relèvent sans aucune hésitation (appels téléphoniques fixes ou mobiles, visio-communications, télécopies, courriers électroniques, messageries instantanées) mais des pratiques comme les listes de discussions ou de diffusion, le chat ou les forums posent plus de difficultés. Pour pouvoir prévenir des interrogations concernant les nouvelles techniques de communication qui apparaîtront certainement dans les prochaines années, on ne peut que recommander au législateur de fixer un critère simple permettant de distinguer celles qui sont susceptibles de faire l'objet d'une interception. Outre le fait que les interceptions ne peuvent concerner que des « correspondances », c'est-à-dire

des communications entre un émetteur et un ou plusieurs destinataires identifiés (et non un contenu simplement stocké sur un serveur), il me semble que ce critère distinctif ne peut être que le caractère privé (ou plus exactement « non public » au sens de la convention de Budapest) de l'échange, autrement dit le fait qu'un tiers ne puisse pas accéder sans autorisation au contenu de cette transmission. En effet, à chaque fois que le mécanisme de communication autorise l'accès (même *a posteriori*) d'un tiers, cette dimension publique ou semi-publique permettra d'aménager à l'autorité publique une autre voie d'accès, moins intrusive au regard des libertés publiques que l'interception.

En termes rédactionnels et dans la perspective d'un toilettage des dispositions du Code de la sécurité intérieure issues de la loi de 1991, on pourrait donc envisager que l'article L. 241-1 du Code de la sécurité intérieure vise explicitement les « correspondances non publiques émises, transmises ou reçues par la voie électronique ».

Mais l'évolution récente des pratiques numériques et des méthodes d'enquête nous conduit également à évoquer le domaine connexe du recueil des métadonnées de connexion, à savoir toutes les informations – autres que son contenu même – qu'engendre l'établissement d'une communication électronique privative et dont la trace est conservée durant une certaine période (une année généralement) par l'opérateur ou l'intermédiaire technique par lequel la communication a été établie. Indirectement visées par l'article L. 244-2 du Code de la sécurité intérieure (qui permet d'obtenir des opérateurs « les informations ou documents qui leur sont nécessaires [...] pour la réalisation et l'exploitation des interceptions autorisées par la loi ») mais dans le but premier de préparer une interception, ces données techniques constituent aujourd'hui une source d'informations extrêmement utile et dont l'exploitation peut parfois être presque aussi fructueuse que celles du contenu des communications. C'est d'ailleurs la raison pour laquelle, la loi du 23 janvier 2006 a introduit à titre expérimental une autre procédure (celle du recours à une « personnalité qualifiée ») permettant aux services du ministère de l'Intérieur l'accès à de telles données aux seules fins de la prévention du terrorisme (article L. 34-1-1 du Code des postes et des communications électroniques).

Cette superposition de deux procédures partiellement redondantes ainsi que les rebondissements récents de l'actualité judiciaire en la matière (en l'occurrence, l'affaire dite des « Fadettes ») nous conduisent à approuver l'opinion émise dans ses derniers rapports par la CNCIS selon laquelle une seule procédure réduirait les difficultés de mise en œuvre et faciliterait le travail de recueil et d'exploitation des données (*cf.* notamment, le rapport 2011-2012 de la CNCIS p. 70). Au-delà même de ces raisons opérationnelles invoquées par la Commission, il nous semble en effet que toute l'évolution de l'économie numérique nous montre que la valeur des données de connexion et de leur traitement est égale voire supérieure à celle du contenu même des communications (et les grands

opérateurs du cyberespace comme Google ou Facebook nous en fournissent un exemple permanent).

Dès lors, sans mettre sur le même plan l'interception de correspondances et la récupération des données techniques de connexion, il serait justifié de fondre ensemble les actuels articles L. 34-1-1 du Code des postes et des communications électroniques et L. 244-2 du Code de la sécurité intérieure dans un nouvel article du même code qui mettrait sous le contrôle de la CNCIS (et dans le cadre d'une procédure adaptée à définir) toutes les demandes effectuées par les services de renseignement et de sécurité touchant aux données techniques de connexion. Il conviendrait alors de s'interroger sur le fait de savoir si ce renforcement du contrôle par la CNCIS ne justifierait pas, en contrepartie, de supprimer la distinction actuellement faite entre le motif de prévention du terrorisme et les autres domaines et d'autoriser sans distinction les demandes de tous les services concernés pour l'ensemble des motifs de sécurité nationale.

Concilier l'usage des interceptions avec l'État de droit

Quel qu'en soit le périmètre, la prérogative régalienne que constitue le recours par l'État aux interceptions de sécurité représente une atteinte réelle à l'exercice des libertés publiques (et particulièrement à la protection de la vie privée, telle qu'elle est garantie constitutionnellement ainsi que par l'article 8 de la CEDH). Il convient donc de s'assurer en permanence qu'un équilibre satisfaisant est établi entre l'intérêt public de sécurité et les garanties des libertés individuelles. C'est à quoi s'attache depuis l'origine le régime instauré par la loi du 10 juillet 1991 dont les principes essentiels ne semblent donc pas à remettre en question, ni le rôle central que joue l'intervention d'une AAI, en l'occurrence la CNCIS.

Tout au plus peut-on tirer de l'expérience des vingt années de pratique et de jurisprudence de la CNCIS quelques enseignements que le législateur pourrait utilement retraduire afin de perfectionner le dispositif.

S'agissant tout d'abord des motifs justifiant le recours aux interceptions, la CNCIS a souvent relevé dans ses rapports annuels la filiation qui existe historiquement entre la rédaction originelle de l'article 3 de la loi de 1991 (aujourd'hui codifié à l'article L. 241-2 du Code de la sécurité intérieure) et celle de l'article 410-1 du Nouveau Code pénal de 1992 qui a défini les « intérêts fondamentaux de la nation ». Par ailleurs, plus récemment, a été établie par le législateur de 2009 la nouvelle notion de « sécurité nationale » (article L. 1111-1 du Code de la défense) que l'article 3 de la loi de 1991 avait, par anticipation, visée sans la définir et que l'article 8 de la CEDH cite également.

Il nous semble que ces trois textes partagent une logique commune. Ce sont en effet les impératifs de la sécurité nationale dont l'État est le garant qui justifient le recours à ce moyen dérogatoire de l'interception de sécurité et qui font l'objet d'une protection pénale particulière. Dès lors, l'objectif d'intelligibilité du droit (souvent rappelé par le Conseil constitutionnel) ainsi que de sa cohérence nous invite à une nouvelle rédaction de l'article 3 qui renverrait explicitement aux deux autres textes du Code pénal et du Code de la défense. Sans vouloir ici se lancer dans un exercice rédactionnel approfondi, on pourrait imaginer que l'article vise désormais les « interceptions justifiées par un motif de sécurité nationale touchant à la protection des intérêts fondamentaux de la nation et en particulier à la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou à la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de l'article L. 212-1 du Code de la sécurité intérieure ». En croisant la sécurité nationale (qui ne serait plus un domaine parmi d'autres, mais le facteur commun qui – comme l'indique le Code de la défense – vise à « identifier l'ensemble des menaces et des risques susceptibles d'affecter la vie de la Nation ») et les domaines couverts par l'article 410-1 du Code pénal, on affirmerait mieux l'exigence d'une motivation en relation directe avec ces seuls intérêts nationaux majeurs (par différence avec les interceptions judiciaires qui peuvent, pour leur part, se prévaloir des motifs de sûreté publique ou de défense de l'ordre et de prévention du crime, également prévus par l'article 8 CEDH) tandis que le rappel des domaines précédemment visés en 1991 préserverait les motifs traditionnels du recours aux interceptions sans exclure tout à fait qu'un autre intérêt fondamental de nation puisse également être invoqué.

Au-delà de la révision des motifs, une autre évolution renforçant l'État de droit paraît aujourd'hui prête à rentrer dans notre droit positif. Il s'agirait de conférer à la commission de contrôle indépendante un réel pouvoir d'autorisation et non plus seulement consultatif. On sait en effet que les avis supposés consultatifs de la CNCIS sont dans leur immense majorité suivis par le Premier ministre et – surtout – qu'en réalité la procédure mise en œuvre n'est plus aujourd'hui une procédure d'intervention *a posteriori* (comme le prévoyait la lettre de la loi de 1991) mais une procédure d'examen *a priori*, laquelle « a transformé *de facto*, le pouvoir de recommandation en un quasi-pouvoir de décision » comme le soulignait l'ancien président Dewost dans le rapport 2011-2012 de la CNCIS (p. 12).

Mettre ainsi le droit en accord avec le fait aurait là encore des avantages de cohérence et de clarté tout en renforçant le caractère incontestable de notre procédure nationale au regard des impératifs toujours plus stricts de la jurisprudence, européenne en particulier. Cela n'empêcherait pas la nouvelle loi de prévoir que le Premier ministre puisse en cas d'urgence et pour un motif d'intérêt national particulier, obtenir un réexamen rapide de la demande et, dans l'intervalle, une suspension

temporaire de la décision de refus d'autorisation. La sécurité nationale et ses impératifs ne seraient donc pas affectés de ce fait mais on aurait ainsi procédé à un rééquilibrage juridiquement et symboliquement important entre la règle (l'autorisation préalable indépendante) et l'exception (la décision discrétionnaire imposée par les circonstances).

Le troisième aspect qui mériterait de retenir l'attention d'un futur législateur pourrait avoir trait à la difficile question de la judiciarisation des interceptions. L'article L. 242-8 du Code de la sécurité intérieure prescrit en effet que « les renseignements recueillis ne peuvent servir à d'autres fins que celles mentionnées à l'article L. 241-2 », ce qui – cumulé avec la classification systématique de toutes les décisions et transcriptions d'interception – empêche, sauf exception, que l'existence et les résultats des interceptions de sécurité puissent être transmis à l'autorité judiciaire et verser en procédure. Certes, cette interdiction est tempérée par le fait qu'elle s'exerce « sans préjudice de l'application du deuxième alinéa de l'article 40 du Code de procédure pénale », ce qui permet aux services concernés de dénoncer au parquet des faits nouveaux susceptibles de révéler la commission d'un délit ou d'un crime. On pourrait cependant souhaiter qu'il soit plus facile à l'autorité administrative d'exploiter judiciairement des résultats de renseignement lorsqu'il s'agit d'un domaine donnant lieu à répression pénale. L'argument qui est souvent opposé à une telle production en procédure tient au fait que ces interceptions n'ont pas le caractère d'un acte de procédure effectué par un officier de police judiciaire et sous le contrôle d'un juge et que la loyauté et la crédibilité d'un tel renseignement pourraient facilement être contestées par la défense. Mais cet argument n'est pas totalement convaincant.

On connaît déjà en effet des cas dans lesquels les résultats d'un acte techniquement couvert par le secret de la défense nationale peuvent être produits en justice : c'est le cas du décryptement de certains fichiers utiles à l'enquête pénale et pour lequel la juridiction concernée choisit de recourir à des moyens couverts par le secret de la défense nationale (articles 230-1 à 230-5 du Code de procédure pénale). Dans un tel cas, est prévue une procédure particulière permettant de concilier le respect du secret et la nécessaire information des juges et des parties. On pourrait donc s'en inspirer pour permettre que la transcription d'une interception de sécurité utile à la justice puisse être déclassifiée (après avis favorable de la CCSDN) et qu'un minimum d'éléments d'information touchant aux conditions d'exécution de l'interception soit communiqué, en respectant les règles fixées par la jurisprudence de la cour de Strasbourg en ce qui concerne le recours aux preuves secrètes.

En conclusion, et pour compléter les différentes pistes de réforme évoquées plus haut, il faut être conscient de ce que la réforme de la loi de 1991 s'inscrira nécessairement dans un mouvement plus vaste de constitution d'un véritable droit de la sécurité nationale, dont la décision fondatrice du Conseil constitutionnel du 10 novembre 2011 (censurant les dispositions de 2009 instaurant une classification de certains lieux,

et non plus seulement des informations qu'ils contiendraient) a marqué sans doute la première étape. Le nouvel équilibre qui s'instaurera entre les nécessités de la sécurité nationale justifiant une interception et la garantie des libertés individuelles aura ainsi valeur de référence pour toutes les autres dispositions légales applicables à l'usage dérogatoire de certains moyens spéciaux par les services d'État ayant une mission de sécurité et de renseignement.

De plus, et si l'on suit les perspectives ouvertes par le rapport parlementaire de la mission d'information de la Commission des lois de l'Assemblée nationale consacrée à l'évolution du cadre juridique applicable aux services de renseignement, cette modernisation du cadre légal des interceptions de sécurité pourrait se doubler d'une extension des missions de la CNCIS afin de faire de cette autorité expérimentée le socle d'un nouveau dispositif de contrôle indépendant des activités des services de renseignement.

De l'interception de correspondances à l'interception de données électroniques ?

Virginie PELTIER
Maître de conférences à l'université-Montesquieu Bordeaux IV, Institut des sciences criminelles et de la justice (EA 4601)

Avec les progrès fulgurants de nouvelles méthodes de communication offrant quasi instantanément d'échanger messages et données d'un endroit à l'autre de la planète, auxquels se sont vite habitués les acteurs la criminalité organisée, les dispositions relatives aux interceptions [1] de correspondances ne suffisent plus à assurer un contrôle efficace des échanges entre délinquants. Les causes sont doubles et tiennent, d'une part, à la relative imprécision de la notion de correspondance [2] et, d'autre part, à la nécessité d'installer dans notre procédure pénale d'autres formes de surveillance, afin d'assurer le contrôle de données non issues de correspondances [3].

1) Judiciaires ou de sécurité.

2) Pour un exemple jurisprudentiel : Cass. crim., 16 oct. 2012 : Bull. crim. n° 216, Comm. com. électr. 2013, n° 29, obs. A. Lepage, Rev. pénit. 2013, p. 377, obs. P. Conte. Voir aussi V. Peltier, *Les enjeux de la protection du secret des correspondances : (bref) bilan et perspectives* : XX^e^ rapport de la CNCIS, 2012, p. 23-28. Les forums, *chats* ou autres échanges sur les réseaux sociaux posent de ce point de vue d'épineuses difficultés, de même que les données techniques de communications, produites à l'occasion d'une correspondance et détenues par les opérateurs de télécommunications (par exemple, nom des correspondants, numéro de la ligne servant à l'appel, durée de la communication, etc.). De même, un enquêteur qui introduit un « mouchard » dans un ordinateur pour capter des données informatiques (CPP, art. 706-102-1s), et prend ainsi connaissance d'un courriel, procède à une interception de correspondance (CPP, art. 100s).

3) Sur la question posée par le recours à la géolocalisation, *cf. infra* n° 4. De même, la récupération de messages réservés sur le compte facebook d'un individu ne peut se fonder sur les articles 100s du Code de procédure pénale, faute de correspondance. Mais elle pourrait s'effectuer grâce à une procédure destinée à permettre d'intercepter ce que l'on pourrait appeler des « données électroniques réservées » (pour désigner des données qui ne sont pas accessibles à tout le monde).

Toutefois, est-il vraiment indispensable d'introduire une nouvelle procédure d'appréhension de telles données dans notre droit ? En effet, aux interceptions judiciaires de correspondances, susceptibles d'être mises en œuvre au stade de l'instruction[1] ou de l'enquête[2] (mais seulement en cas de criminalité organisée), s'ajoutent déjà, sur décision d'un juge d'instruction et uniquement dans le cadre de la lutte contre la criminalité organisée, la sonorisation et la fixation d'images de certains lieux ou véhicules[3] ainsi que la captation de données informatiques[4], ces dernières faisant aussi l'objet, en droit commun, de mesures destinées à permettre aux enquêteurs d'y avoir accès et de les copier en phase d'enquête[5] comme d'instruction[6].

Il est en définitive deux manières d'aborder la question. En premier lieu, le législateur peut choisir de préciser le régime juridique de chaque mesure de surveillance qu'il souhaite introduire dans notre droit. Conforme au principe de la légalité criminelle[7], le procédé présente deux inconvénients techniques : d'une part, la loi est susceptible d'être – à plus ou moins longue échéance – dépassée par les évolutions technologiques et, de ce fait, inefficace, d'autre part, les impératifs de l'enquête « proactive »[8] risquent de mal s'accommoder d'une description trop détaillée des opérations susceptibles d'être mises en œuvre.

On peut alors, en second lieu, concevoir une procédure élargie d'appréhension des données électroniques qui ne reposerait que sur leur caractère réservé, sans plus d'égard pour leur nature juridique (s'agit-il de correspondances ? de données informatiques ? de propos échangés dans certains lieux ou véhicules ? d'un autre type de données ?), qui conditionne le déclenchement d'un mécanisme de surveillance précis au régime juridique spécifique. Cette solution, qui prend quelques libertés avec le principe de légalité criminelle, présente en revanche l'avantage d'être plus pragmatique puisqu'elle a vocation à englober de multiples opérations de surveillance, sans qu'il soit besoin que le détail de leur mise en œuvre apparaisse au grand jour.

En résumé, la difficulté est de résoudre un conflit entre, d'un côté, les impératifs de la légalité criminelle, rempart protégeant les citoyens contre des intrusions étatiques dans leur vie privée qui pourraient se révéler abusives, et, d'un autre, le souci d'efficacité des autorités publiques pour lutter contre le terrorisme ou, entre autres, les trafics de toute nature. Quoi qu'il en soit, si l'on se range à l'idée d'une interception

---

1) Code de procédure pénale, art. 100 s.
2) Code de procédure pénale, art. 706-95.
3) Code de procédure pénale, art. 706-96 s.
4) Code de procédure pénale, art. 706-102-1 s.
5) Code de procédure pénale, art. 57-1 (flagrance), 76-3 (préliminaire).
6) Code de procédure pénale, art. 97-1.
7) *Cf. infra* nº 4s.
8) Chrisje Brants et Stewart Field, Les méthodes d'enquête proactive et le contrôle des risques : déviance et société 1997, vol. 21, p. 401s.

de données électroniques, deux questions doivent être abordées : celle de sa conformité aux exigences juridiques et celle de ses modalités.

Conformité de l'interception de données électroniques

Conformité au droit interne. En procédure pénale, tout ce qui n'est pas autorisé est interdit – par respect pour les libertés individuelles –, de sorte qu'il est impératif que le législateur intervienne pour préciser le champ des investigations autorisées sur les données électroniques. Partant, le contrôle de la CNCIS ne peut normalement porter que sur une technique de surveillance préalablement régie par la loi.

Une disposition générale est par définition peu conforme aux exigences d'une légalité – formelle[1] comme matérielle – qui ne se satisfait guère de libellés imprécis et exige que le contenu de la règle permette son application prévisible pour le justiciable. La première difficulté, qui ne peut relever que de l'arbitrage du législateur, en la matière serait d'ailleurs de définir ce que l'on entend par « données électroniques réservées » afin de circonscrire le champ d'intervention des enquêteurs. De même, en fonction des opérations de surveillance envisagées, il conviendra de préciser les modalités d'appréhension des données (interception ? captation ? enregistrement ?).

Une règle trop imprécise risque de ne pas franchir l'écueil du contrôle constitutionnel, *a priori* ou *a posteriori*, quoique le conseil et la Cour de cassation[2] considèrent, à l'aune de la CEDH[3], que le juge pénal, en interprétant la loi, peut la rendre conforme aux exigences de la légalité.

Conformité au droit européen. Pour la CEDH, la question est simple : la mesure de surveillance constitue-t-elle une ingérence dans la vie privée ou la correspondance ? Dans l'affirmative, et pour qu'elle soit justifiée, cette ingérence est-elle prévue par la loi et nécessaire dans une société démocratique ?

Sur le point de savoir si une interception de données électroniques pourrait constituer une ingérence, il ressort de la jurisprudence de la Cour

---

1) Quoique la Cour de cassation ait admis la validité de la géolocalisation sur le fondement de l'article 81 Code de procédure pénale selon lequel le juge d'instruction procède à tous les actes d'information qu'il juge utiles à la manifestation de la vérité, oubliant qu'il est précisé qu'il doit le faire « conformément à la loi ». Pareille motivation avait déjà valu à la France une condamnation européenne en matière d'écoutes téléphoniques…

2) *Cf.*, par ex., Cass. crim., 10 avr. 2013, nº 12-85618 ; 16 avr. 2013, nº 13-90010 ; 16 avr. 2013, nº 13-90008 ; 14 mai 2013, nº 13-9000528 mai 2013, nº 12-87266.

3) Cf., par ex., CEDH, *Uzun c. All*, 2 septembre 2010, nº 35623/05, §62.

que l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales implique de pouvoir nouer des relations avec autrui, en privé ou au sein du domaine public[1], de sorte qu'il y a de fortes chances qu'une interception de données échangées entre des personnes[2], même sur des réseaux publics, constitue une ingérence au sens de l'article 8 de la Convention.

Pour la justifier il faut alors se demander, d'abord, si elle est prévue par la loi : ici, la réponse est à chercher dans l'arrêt du 2 septembre 2010 *Uzun c. Allemagne*[3], relatif à l'utilisation d'un procédé de géolocalisation, dans lequel la Cour européenne indique qu'en matière de surveillance secrète, la loi, qui doit être particulièrement précise eu égard aux risques d'abus, doit, en termes clairs, indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à recourir à de telles mesures[4]. Toutefois, elle laisse une marge de manœuvre à l'interprétation judiciaire pour compléter le dispositif en vigueur.

S'agissant du fond, le droit interne doit offrir une protection contre les ingérences arbitraires en développant diverses garanties afférentes à la nature, l'étendue, la durée de la mesure envisagée, les raisons requises pour l'ordonner, l'autorité compétente pour y recourir[5], son exécution et son contrôle ou, entre autres, les types de recours offerts au justiciable.

Enfin, il faut s'interroger sur la nécessité de recourir à ce type de procédé dans une société démocratique, le but poursuivi devant d'ailleurs être légitime. On pourra alors se référer aux motifs de l'opération : la personne est soupçonnée d'une infraction extrêmement grave ou, dans des circonstances très limitées, la cour admet même qu'un tiers puisse être visé parce que soupçonné lui-même d'être en rapport avec l'accusé[6].

---

1) Pour la cour, la collecte et la conservation systématiques d'informations par des services de sécurité sur certains individus, même sans recours à des méthodes de surveillance secrète, constituent une ingérence dans la vie privée de ces personnes : CEDH, *Rotaru c. Roumanie* [GC], 4 mai 2000, nº 28341/95 ; *P. G. et J. H. c. RU*, 25 septembre 2001 ; *Peck c. RU*, 28 janv. 2003, nº 44647/98 ; *Perry c. RU*, 17 juillet 2003, nº 63737/00.
2) Que la loi qualifiera, de surcroît, de « réservées ».
3) CEDH, *Uzun c. All*, 2 septembre 2010, nº 35623/05.
4) CEDH, *Uzun c. All*, préc., § 61.
5) L'intervention ou le contrôle par un juge étant évidemment un élément favorable : CEDH, *Uzun c. All*, préc., § 71.
6) CEDH, *Uzun c. All*, préc., § 70.

Modalités de l'interception de données électroniques

L'interception judiciaire de données électroniques. Sa procédure peut être calquée sur celle des interceptions de correspondances : ordonnée en matières criminelle et correctionnelle, par un juge d'instruction ou, au stade de l'enquête en matière de criminalité organisée, autorisée et contrôlée par le juge des libertés et de la détention, après requête du procureur de la République, elle ferait l'objet d'une décision écrite qui comporterait tous les éléments d'identification de la liaison à intercepter, l'infraction qui la justifie et sa durée, éventuellement renouvelable. Le juge d'instruction ou le procureur de la République pourrait requérir tout agent qualifié d'un service ou organisme placé sous l'autorité ou la tutelle du ministre chargé des Télécommunications ou tout agent qualifié d'un exploitant de réseau ou fournisseur de services de télécommunications autorisé pour procéder à l'installation du dispositif d'interception.

La modification à apporter par rapport à l'interception de correspondance serait d'autoriser les enquêteurs à intercepter, enregistrer ou transcrire les données électroniques, sans que ces trois opérations soient indéfectiblement liées pour permettre un élargissement des moyens d'investigation [1]. Par exemple, si l'on considère que les données issues de la géolocalisation d'un individu constituent des données électroniques [2], les enquêteurs qui les exploitent ne les ont pas interceptées, mais ils vont procéder à leur enregistrement et à leur transcription. Si ces deux dernières opérations devaient dépendre d'une interception préalable, les règles nouvelles ne pourraient recevoir application, faute d'interception.

L'interception de sécurité de données électroniques. Ici aussi, il ne s'agirait que de reprendre, peu ou prou, les modalités des interceptions de correspondances en les adaptant aux données électroniques. Sur proposition écrite et motivée du ministre de la défense, du ministre de l'Intérieur ou du ministre chargé des Douanes et accordée par décision écrite et motivée du Premier ministre – centralisant l'exécution de toutes les interceptions autorisées –, elle serait donnée, pour une durée déterminée, afin de répondre à l'un des objectifs poursuivis par ces interceptions : rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées.

---

1) Le problème s'était posé lorsque des policiers avaient recopié des messages parvenus sur les récepteurs de messagerie unilatérale d'un prévenu : pour la Cour de cassation, il n'y avait pas eu d'interception puisque les messages étaient parvenus à destination (Cass. crim., 14 avr. 1999 : Bull. crim. nº 82, JCP 2000, II, 10312). En revanche, ils avaient bel et bien été transcrits…

2) C'est au législateur qu'il reviendra de poser une définition des données à intercepter pour délimiter le domaine d'application des interceptions : *cf. supra* nº 4.

Rôle de la Commission nationale de contrôle des interceptions de sécurité. Elle poursuivrait ses mêmes missions, tout d'abord, en donnant son accord à l'interception – plutôt que son avis –[1] puis en établissant diverses recommandations sur le contingent et la répartition des interceptions entre les différents ministères ou en procédant au contrôle de toute interception de sécurité en vue de vérifier si elle est effectuée dans le respect des règles légales, de sa propre initiative ou sur réclamation de toute personne y ayant un intérêt direct et personnel.

1) Puisque, semble-t-il, telle est déjà la pratique en vigueur.

Première partie

RAPPORT D'ACTIVITÉ

Chapitre I

Organisation et fonctionnement de la Commission

Composition de la Commission

À la date de rédaction du présent rapport, la composition de la Commission est la suivante :

Membres de la Commission

- Hervé PELLETIER, président de chambre honoraire à la Cour de cassation, nommé pour une durée de six ans par le Président de la République – décret du 3 octobre 2009, publié au *Journal officiel* le 4 octobre 2009.
- Membre parlementaire – Sénat : Jean-Jacques HYEST, sénateur (UMP) de Seine-et-Marne, désigné le 6 décembre 2011 par le président du Sénat.
- Membre parlementaire – Assemblée nationale : Jean-Jacques URVOAS, député (PS) du Finistère, désigné le 23 juillet 2012 par le président de l'Assemblée nationale.

La Commission est assistée de deux magistrats de l'ordre judiciaire :

- Olivier GUÉRIN, délégué général, depuis sa nomination en date du 8 septembre 2011.
- Loïc ABRIAL, chargé de mission, depuis sa nomination en date du 15 mars 2012.

Le secrétariat est assuré par Nathalie Brucker et Marie-José Masset.

Christophe Germin est l'officier de sécurité du service et conduit le véhicule de la Commission.

Rappel des compositions successives de la Commission

Présidents :

- Paul Bouchet, conseiller d'État, 1er octobre 1991.
- Dieudonné Mandelkern, président de section au Conseil d'État 1er octobre 1997.
- Jean-Louis Dewost, président de section au Conseil d'État, 1er octobre 2003.
- Hervé Pelletier, président de chambre à la Cour de cassation, 3 octobre 2009.

Représentants de l'Assemblée nationale :

- François Massot, député des Alpes-de-Haute-Provence, 19 juillet 1991.
- Bernard Derosier, député du Nord, 24 mai 1993.
- Jean-Michel Boucheron, député d'Ille-et-Vilaine, 3 juillet 1997.
- Henri Cuq, député des Yvelines, 4 juillet 2002.
- Bernard Derosier, député du Nord, 20 mars 2003.
- Daniel Vaillant, député de Paris, 1er août 2007.
- Jean-Jacques Urvoas, député du Finistère, 23 juillet 2012.

Représentants du Sénat :

- Marcel Rudloff, sénateur du Bas-Rhin, 17 juillet 1991.
- Jacques Thyraud, sénateur du Loir-et-Cher, 26 mars 1992.
- Jacques Golliet, sénateur de Haute-Savoie, 22 octobre 1992.
- Jean-Paul Amoudry, sénateur de Haute-Savoie, 14 octobre 1995.
- Pierre Fauchon, sénateur du Loir-et-Cher, 18 septembre 1998.
- André Dulait, sénateur des Deux-Sèvres, 6 novembre 2001.
- Jacques Baudot, sénateur de Meurthe-et-Moselle, 26 octobre 2004.
- Hubert Haenel, sénateur du Haut-Rhin, 4 juillet 2007, en remplacement du sénateur Jacques Baudot décédé, puis le 15 octobre 2008 en qualité de membre parlementaire de la Commission, à titre personnel.
- Jean-Jacques Hyest, sénateur de Seine-et-Marne, nommé le 2 juin 2010 en remplacement du sénateur Hubert Haenel, nommé membre du Conseil constitutionnel, puis le 6 décembre 2011, à titre personnel.

Missions et fonctionnement

La Commission est chargée de veiller au respect des dispositions du Titre IV du Livre II du Code de la sécurité intérieure consacré aux « interceptions de sécurité ». En effet, l'ordonnance n°2012-351 du 12 mars 2012 a abrogé la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques depuis le 1er mai 2012, et a rassemblé l'essentiel de ses dispositions à droit constant au sein du Code de la sécurité intérieure.

Conformément à l'article 1er de son règlement intérieur, « la Commission se réunit à intervalles réguliers à l'initiative de son président ; elle peut également être réunie à la demande d'un de ses membres ».

Entre ces assemblées plénières, le président dispose d'une habilitation permanente à l'effet de formuler les avis, les recommandations et les préconisations, dès lors que les demandes présentées, d'interception ou de recueil de données techniques de communications, ne posent pas de questions nouvelles par rapport aux délibérations et aux décisions précédentes de la Commission dans sa formation plénière.

Elle peut à tout moment adresser au Premier ministre une recommandation tendant à ce qu'une interception soit interrompue. Elle peut également faire une recommandation d'avertissement pour alerter le Premier ministre sur des difficultés, qui en perdurant ou en se développant, pourraient fonder un avis d'interruption de la part de la Commission ou de non-renouvellement de la mesure. Des préconisations sont également adressées aux services titulaires de l'autorisation et en charge de l'exploitation du renseignement, avant la procédure de recommandation.

En application de l'article L. 243-9 du Code de la sécurité intérieure (ancien article 15 de la loi de 1991), la Commission reçoit les réclamations des particuliers, procède aux contrôles et aux enquêtes qui lui paraissent nécessaires à l'accomplissement de sa mission. À la demande des particuliers, la Commission effectue les vérifications dans le cadre du contrôle des interceptions de sécurité ordonnées par le Premier ministre pour les motifs prévus par la loi et réalisées par les services habilités. Les investigations de la Commission portent exclusivement sur l'existence ou non d'interceptions illégales qui auraient été conduites par des services de l'État habilités, et ce en violation des dispositions issues de la loi du 10 juillet 1991 relative au secret des correspondances et de la vie privée.

En vertu du même article, la Commission peut procéder à son initiative aux vérifications qu'elle estime nécessaires pour s'assurer que l'interception de sécurité est bien effectuée selon les conditions prévues par la loi et par la décision d'autorisation. Ainsi près de 25 % des interceptions font l'objet d'un contrôle direct et en temps réel de leur exploitation.

En outre, la Commission, ou par délégation de celle-ci son président, peut ordonner les vérifications qui lui paraissent nécessaires à la suite d'informations ou de déclarations publiques de personnes faisant état d'interceptions de leurs communications électroniques ou des données techniques se rattachant à celles-ci.

À l'occasion de ces différents contrôles et dans l'hypothèse où la Commission constaterait une violation des dispositions légales en matière d'interceptions et de recueil de données techniques, elle doit adresser un avis sans délai au procureur de la République en application de l'article 40 du Code de procédure pénale.

En revanche, la Commission ne procède à aucune investigation sur les interceptions ordonnées par l'autorité judiciaire, qui relèvent du seul contrôle de cette même autorité, en application des dispositions du Code de procédure pénale. De même, les interceptions qui seraient faites par des particuliers sont de la compétence exclusive des services judiciaires territorialement compétents pour recevoir ces plaintes. Hors du champ de compétence de la CNCIS, les requêtes des particuliers qui portent sur ces interceptions présumées ou réelles sont déclarées irrecevables.

La Commission contrôle les conditions d'exécution des mesures autorisées par le Premier ministre. À ce titre, elle se rend auprès des services et des directions titulaires des autorisations et en charge de l'exécution des mesures de renseignement portant sur les communications électroniques. Conformément à l'article L. 243-10 du Code de la sécurité intérieure (ancien article 16 de la loi de 1991), les ministres, autorités publiques et agents publics doivent prendre toutes mesures de nature à faciliter son action. Ainsi une vingtaine de sites où sont mis en œuvre ces mesures et exploitées le renseignement technique sont visités par les agents de la Commission au cours d'une année.

La CNCIS est en outre chargée, en application de l'article 6 de la loi n° 2006-64 du 23 janvier 2006 relative à la loi contre le terrorisme, du contrôle des demandes de communication des données prévues par l'article L. 34-1-1 du Code des postes et des communications électroniques. Ce sont les demandes formées, pour la prévention des actes de terrorisme, par les services habilités du ministère de l'Intérieur.

Toutes les autres demandes relatives au recueil des données techniques de communications sont formulées par les services habilités des ministères de l'Intérieur, de la Défense et des Finances et traitées par le groupement interministériel de contrôle (GIC). Elles relèvent de l'article L. 244-2 du Code de la sécurité intérieure (ancien article 22 de la loi du 10 juillet 1991) et sont soumises, dans les mêmes conditions que l'article 6 de la loi du 23 janvier 2006, au contrôle de l'autorité administrative indépendante.

La CNCIS est membre de la Commission consultative créée par le décret n° 97-757 du 10 juillet 1997 qui, sous la présidence du directeur

général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), émet des avis sur les demandes de commercialisation, d'importation, d'acquisition, de détention ou d'emploi des matériels susceptibles de porter atteinte au secret des correspondances.

En application de l'article L. 243-7 du Code de la sécurité intérieure, le président remet au Premier ministre, avant publication, un rapport annuel sur les conditions d'exercices et les résultats de l'activité de la Commission. Les présidents des deux assemblées en sont également destinataires.

Financement

Autorité administrative indépendante, la CNCIS dispose de crédits individualisés figurant au budget des services du Premier ministre. Le président est ordonnateur des dépenses (article L. 243-6 du Code de la sécurité intérieure).

Pour l'année 2012 et conformément à la déclinaison en programmes, actions et sous actions de la loi organique relative aux lois de finances (LOLF), le budget de la CNCIS a été inscrit au sein du programme 308 « protection des droits et libertés ».

Afin de garantir son indépendance budgétaire, la Commission est dotée d'un budget opérationnel de programme (BOP), référencé 308AIC.

Les crédits alloués en 2012 se sont élevés à 607 803 euros (619 897 euros en 2011) dont 529 864 euros (523 619 euros en 2011) pour les dépenses du Titre II (dépenses de personnel) et 77 939 euros (96 278 euros en 2011) pour les dépenses de fonctionnement.

Le budget global de la CNCIS a donc connu une diminution de 12 094 euros (environ 2 %, hors inflation). Cette tendance à la baisse se poursuivra en 2013. Les crédits alloués auraient dû être de 553 947 euros dont 474 474 pour les dépenses du Titre II (dépenses de personnel) et 79 473 pour les dépenses de fonctionnement. Les mesures budgétaires adoptées au cours de l'année ont entraîné une baisse de 1 % de ce montant soit 77 199 euros. Le budget des dépenses du Titre II relatif au personnel est lui en nette diminution, la CNCIS passant de six à cinq ETPT. Cette évolution du plan des effectifs interdit, en l'état, toute possibilité de recrutement, qui pourrait s'avérer nécessaire avec l'accroissement des missions de contrôle de la Commission.

Ces actions de maîtrise des dépenses publiques mises en œuvre par la CNCIS depuis plusieurs années trouvent désormais leur limite.

Depuis 1991, les prérogatives de la Commission ont été accrues à plusieurs reprises. Chargée du contrôle de l'exécution des écoutes, elle a

très vite été sollicitée pour adresser des avis préalables sur chaque projet d'interception.

En 1997, elle est devenue membre de la commission consultative placée auprès du Premier ministre pour délivrer les autorisations de fabrication, d'importation, d'exposition, d'offre, de location, de vente, d'acquisition ou de détention de matériels permettant de porter atteinte à l'intimité de la vie privée ou au secret des correspondances.

En 2006, elle a reçu pour tâche de contrôler les demandes de données techniques de communications, dont le nombre est au moins dix fois supérieur à celui des demandes d'interceptions de sécurité. Les modalités des vérifications de ces demandes ont été renforcées en 2010 aux fins d'adapter le recueil de ces renseignements aux enjeux de sécurité et de protection des données de communications privées. Depuis lors, la Commission assure le contrôle systématique et constant des demandes validées, tant par la personnalité qualifiée pour les demandes des services du ministère de l'intérieur habilités en matière de lutte contre le terrorisme, que par le GIC pour les demandes des services habilités au titre de la loi du 10 juillet 1991 et portant sur les différents motifs autorisant l'interception des communications.

Les mesures de géolocalisation en temps réel sont susceptibles d'être placées sous le contrôle de la CNCIS dès l'entrée en vigueur de la loi de programmation militaire.

Dans ce contexte d'élargissement des compétences de la Commission, les baisses budgétaires annuelles sont de nature à remettre en cause partiellement la nature et la périodicité des contrôles de l'AAI. La CNCIS a ainsi dû reporter des visites de contrôle, faute de disposer de financement suffisant.

En effet, les crédits du BOP CNCIS sont destinés en priorité à permettre le fonctionnement continu de la CNCIS, en toute sécurité. Ainsi la structure permanente de la Commission comprend, outre le président, deux magistrats et deux secrétaires fonctionnant en binômes. La Commission doit pouvoir être jointe et s'entretenir avec ses interlocuteurs de façon sécurisée. Ses locaux sont équipés pour répondre aux normes relatives au traitement des documents classifiés au niveau « secret-défense ». Elle doit accéder aux moyens d'information les plus larges comme les plus spécialisés en source ouverte. Elle doit également disposer de moyens de transport dédiés et sécurisés, notamment pour le transfert des documents classifiés et pour effectuer les visites de contrôle prévues par la loi.

La CNCIS participe aux travaux menés par les services du Premier ministre sur la mesure de la performance en matière de gestion budgétaire. Elle poursuit donc, depuis 2009, des actions de rationalisation financière. Ainsi de nouveaux indicateurs de performance ont été élaborés pour couvrir l'intégralité de ses activités, tant celles portant sur

l'expertise fournie pour la prise de décision des autorités publiques, que celles destinées à garantir la protection des droits et libertés des citoyens, attribuées par le législateur à l'AAI.

Dans le même souci d'efficacité et de lisibilité de son activité, la Commission a choisi de mettre en œuvre le dispositif de contrôle interne des services du Premier ministre prévu par le décret n°2011-775 du 28 juin 2011 relatif à l'audit interne dans l'administration et mis en place progressivement depuis le début de l'année 2012.

Elle s'inscrit pleinement dans la démarche de modernisation de l'action publique définie par la circulaire du Premier ministre du 7 janvier 2013 et visant à l'élaboration d'un plan de modernisation et de simplification de l'action publique destinés à améliorer le service aux citoyens, l'organisation et le fonctionnement des services, ainsi que la mutualisation des fonctions support. Ainsi la Commission a décidé, au-delà des actions internes, de participer au comité de pilotage de ce plan et de s'associer notamment aux programmes « ouverture et partages des données publiques » « accueil et traitement des demandes des requérants » ou « projet de mutualisation et immobilier Ségur des AAI et des SPM ».

La CNCIS prend toute sa part dans l'effort collectif de rationalisation des dépenses publiques. Elle poursuit sa recherche d'économies, notamment sur le plan du fonctionnement. Néanmoins, l'extension de ses attributions et des saisines ainsi que les exigences techniques et matérielles du contrôle dans ces domaines en évolution constante et rapide, nécessitent de disposer de moyens adaptés aux objectifs de protection des libertés publiques et de sécurité, dévolus par le législateur à la Commission. Les crédits sollicités par la CNCIS pour le prochain exercice budgétaire résultent de ce constat. À défaut de prise en compte de cette demande, la Commission devra revoir l'étendue de ces contrôles et des garanties qui y sont attachées.

Relations extérieures

Dans le prolongement des travaux avec les autorités bulgares, allemandes, belges et roumaines, déjà évoqués dans les précédents rapports d'activité, la Commission a poursuivi ses échanges avec les institutions et les structures de pays étrangers dont les compétences rejoignent en partie ou en totalité ses attributions.

Sur la période 2012-2013, trois délégations ont été accueillies à la CNCIS.

• Une délégation libanaise, conduite par le président du Conseil d'État, M. Choucri Sader, a été reçue en août 2012 pour traiter des évolutions législatives et réglementaires en France et au Liban en matière de communications électroniques. Durant les échanges, ont principalement

été évoquées la réglementation en matière de données techniques de communications, les conditions juridiques de leur recueil et de leur exploitation par les services de renseignement, ainsi que les modalités des contrôles réalisés par l'autorité administrative indépendante. M. Choucri SADER a pu rappeler que la démarche des autorités libanaises visait à adapter une législation nationale inspirée à l'origine par la loi française du 10 juillet 1991.

• Une délégation canadienne a été reçue en mars 2013. Elle était conduite par Mme Marie-Hélène CHAYER, directrice des politiques sur les technologies d'enquête et les télécommunications, au sein de la Direction générale des opérations de la sécurité nationale du ministère de la Sécurité publique du Canada. Les discussions ont notamment porté sur l'évaluation des systèmes légaux de contrôle des matériels permettant de porter atteinte à l'intimité de la vie privée ou au secret des correspondances, ainsi que sur les obligations légales des opérateurs en communications électroniques.

• Une délégation turque, représentant la division de suivi et de surveillance technique du ministère de l'Intérieur et chargée d'une étude sur les dispositifs des pays de l'Union européenne, a été reçue en octobre 2013 pour échanger sur les organes et les procédures de contrôle, ainsi que sur la législation relative aux matériels d'interceptions des communications électroniques.

Ces travaux bilatéraux et les projets législatifs exposés par les délégations étrangères, montrent une préoccupation commune d'évolution du cadre légal régissant le recueil administratif ou judiciaire du renseignement technique. Ils témoignent de problématiques et de travaux similaires sur les données techniques de communications avec des questions portant sur leur accès (général ou individualisé, aléatoire ou ciblé), sur la détermination de leur régime et sur les modalités du contrôle de ces recueils par les services d'État et les opérateurs privés.

Les agents de la Commission ont poursuivi les actions de formation et les études conduites avec plusieurs organismes d'enseignement et de recherche, telles que la participation à un groupe de travail sur les pratiques des services de renseignement et les libertés publiques au sein des instituts d'études politiques, les interventions dans le cadre de la formation continue des magistrats de l'ordre judiciaire sur le traitement judiciaire du renseignement, de la formation initiale des commissaires de police sur le recueil du renseignement technique issu des communications électroniques, ou les conférences auprès d'organismes comme l'Institut des hautes études de la défense nationale, ainsi que dans les cycles de formation de l'Académie du renseignement.

Chapitre II

Actualités de la Commission au cours de l'année 2012-2013

Au cours de l'année 2012-2013, la CNCIS a connu une actualité riche. À l'occasion de ce rapport public, il convient de revenir sur deux thèmes essentiels qui sont, d'une part, les perspectives d'avenir de la CNCIS à la lumière de l'évolution du cadre légal du renseignement et, d'autre part, la déclassification de données en rapport avec les interceptions de sécurité.

Perspectives et enjeux relatifs à l'évolution du cadre légal des interceptions et du renseignement

Après vingt-deux ans d'exercice, la CNCIS a démontré qu'elle avait pleinement investi la mission de contrôle que lui a confiée le législateur en 1991. Les chiffres de son activité dans ce rapport 2012-2013 en témoignent.

La CNCIS a su faire face, à travers l'évolution de ses avis et recommandations, au défi de l'innovation permanente dans le domaine des technologies de communication électronique, pour garantir un contrôle de l'ensemble des mesures attentatoires aux libertés et protéger ainsi le secret des correspondances. Son champ d'intervention, comme les modalités dont elle use pour effectuer ses contrôles, ont ainsi confirmé la spécificité de son rôle au sein des AAI comme auprès des services de renseignement.

Comme le rappelaient déjà les rapports publics des années précédentes, la « jurisprudence » de la Commission a su s'adapter depuis plus de deux décennies aux changements majeurs ayant affecté le domaine des communications électroniques. Mais si elle constitue indéniablement une source d'inspiration voire de production du droit, elle n'est pas la loi. C'est désormais à cette dernière d'entrer dans une phase d'adaptation rendue nécessaire par les évolutions des technologies, des comportements en matière de communications, et des nouveaux risques pesant tant sur les individus que sur la collectivité nationale.

Face à des menaces d'atteintes aux intérêts fondamentaux de la Nation de plus en plus transversales, qualifiées par les services judiciaires et de renseignement de « multi-cartes », avec des objectifs qui mêlent souvent des aspects de la criminalité organisée, des atteintes à la sécurité nationale et même parfois du terrorisme, confronté au développement constant des technologies de communications et des utilisations frauduleuses plus ingénieuses que tentent d'en faire les cybercriminels, le texte issu de la loi du 10 juillet 1991 rencontre depuis quelques années certaines limites.

Au regard de ces éléments et des dispositions constantes du droit européen, il apparaît incontournable que, sans plus attendre, la législation en matière d'interceptions de sécurité et de recueil de données techniques de communications soit revue, complétée et modernisée.

L'ordonnance du 12 mars 2012, relative à la partie législative du Code de la sécurité intérieure, a abrogé, depuis le 1er mai 2012, la loi du 10 juillet 1991 dont les dispositions portant sur la police administrative ont été intégrées dans le Code de la sécurité intérieure. Cette codification, quasi exclusivement à droit constant, ne répond pas aux attentes réformatrices que porte la CNCIS.

Les récents travaux consacrés à l'avenir du renseignement, comme le Livre blanc sur la défense et la sécurité nationale rendu public le 29 avril 2013, le rapport de la mission parlementaire sur l'évaluation du cadre juridique applicable aux services de renseignement déposé le 14 mai 2013 et le rapport de la commission d'enquête sur le fonctionnement des services de renseignement français dans le suivi et la surveillance des mouvements radicaux armés déposé le 24 mai 2013, ont eux aussi mis l'accent sur la nécessité de moderniser et de renforcer le cadre légal dans lequel doit s'exercer l'action des services de renseignement.

Dans leur analyse relative aux moyens dédiés au renseignement technique, les auteurs du rapport du 14 mai 2013 ont manifesté le souci de préserver l'équilibre entre la sécurité de l'État et la liberté des citoyens, socle de la loi du 10 juillet 1991 aujourd'hui codifiée. Comme l'a d'ailleurs rappelé Jean-Jacques Urvoas : « Aucun moyen ne peut être octroyé aux

services de renseignement sans qu'un contrôle démocratique s'assure de son usage démocratique, légal et proportionnel[1]. »

Or, il est constant que les services sollicitent de nouveaux moyens d'enquête pour remplir leurs missions de renseignement, qui sont de nature à porter atteinte à certaines libertés publiques. Le rapport préconise de doter les services de nouveaux outils, déjà employés dans le cadre judiciaire des lois dites « Perben II »[2] et « LOPPSI II »[3] : infiltration, sonorisation, captation d'images ou de données informatiques.

Ces techniques spéciales d'enquêtes qui figurent déjà dans le Code de procédure pénale, mais également d'autres moyens d'investigations comme la géolocalisation en temps réel, paraissent devoir être intégrés dans le Code de la sécurité intérieure, au titre de la police administrative du renseignement et de la prévention des atteintes les plus graves. Mettant en cause des libertés publiques et des droits individuels, elles pourraient s'inscrire dans un cadre similaire à celui des interceptions de sécurité.

En application du droit européen et conformément au cadre existant sur le plan judiciaire, ces nouveaux moyens d'investigations nécessitent un contrôle efficient et indépendant des institutions en charge de leur mise en œuvre. Les auteurs du rapport parlementaire du 14 mai 2013 préconisent que la CNCIS serve de base à la création d'une AAI qui aurait des compétences élargies : cette Commission s'assurerait du respect des principes de légalité et de proportionnalité dans l'usage par les services de renseignement des moyens techniques de collecte d'informations.

La CNCIS démontre en effet depuis 1991 qu'une autorité administrative indépendante permet de concilier protection de la vie privée et efficacité des services. Pour autant, l'efficience de ce contrôle et le respect de ses préconisations sont le résultat d'un savant dosage tant dans la composition du collège de ses membres que dans le choix des agents qui la représentent.

Une composition majoritairement parlementaire

Le législateur de 1991 a veillé à ce que l'assemblée plénière de la CNCIS soit composée au deux tiers de parlementaires. Cette présence majoritaire de membres du Parlement, issus à parité de l'Assemblée nationale et du Sénat, comme le prévoit la loi, a été renforcée par une pratique non remise en cause à ce jour : la représentation paritaire de la majorité et de l'opposition. Cette coutume est un facteur déterminant de

1) *Le Point*; 10 juin 2013.
2) Loi nº 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.
3) Loi nº 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

l'indépendance de la Commission. Les regards croisés de représentants du Sénat et de l'Assemblée nationale qui relèvent de groupes politiques distincts, confortent la neutralité de l'action de la Commission et sa transparence vis-à-vis de la représentation nationale dans l'accomplissement de ses missions de vérification.

La CNCIS est par ailleurs présidée par un haut magistrat, de l'ordre administratif ou judiciaire, dont le mandat, tout comme celui des parlementaires, n'est pas renouvelable. Cette garantie renforce l'indépendance de l'institution, ainsi que le démontrait le président Jean-Louis Dewost dans le 20e rapport de la Commission [1].

Des agents de la Commission, magistrats de l'ordre judiciaire détachés auprès d'elle

Depuis 1991, la CNCIS a toujours compté parmi ses agents des magistrats de l'ordre judiciaire, chargés notamment des contrôles effectués chaque jour, en application des instructions fixées par l'assemblée plénière. Leur statut de magistrats détachés et leur expérience juridictionnelle se sont avérés des atouts décisifs pour veiller à la bonne articulation entre les phases administrative et judiciaire, pour traiter la grande majorité des demandes soumises à l'examen de la CNCIS (terrorisme et criminalité et délinquance organisées, représentent 70 % des interceptions de sécurité qui correspondent aux domaines naturels de compétence des magistrats de l'ordre judiciaire, et pour mettre en œuvre les mesures de protection des libertés publiques, dont l'autorité judiciaire est la garante constitutionnellement.

Si, comme le constatent les auteurs du rapport du 14 mai 2013, la CNCIS peut être qualifiée de « modèle abouti » [2], c'est par la mise en œuvre des dispositions de la loi par les parlementaires et les magistrats, membres et agents de cette Commission, qui ont su garantir depuis deux décennies l'indépendance, l'impartialité, la compétence et l'autorité dont doit faire preuve cette institution.

Ce « modèle » doit conserver les atouts conférés par la loi. Il doit également prendre en compte les pratiques et les avis qui ont consolidé et amplifié les apports de la loi.

Ainsi, il convient de consacrer la pratique constante d'une représentation de la majorité et de l'opposition parlementaire au sein de l'assemblée plénière de la CNCIS, comme d'inscrire dans la loi le principe de l'avis *a priori* de la Commission pour tout projet d'interception de sécurité, mécanisme mis en œuvre dès la création de l'AAI.

---

1) Rapport d'activité 2011-2012 p. 9 à 13.
2) Rapport de la mission parlementaire sur l'évaluation du cadre juridique applicable aux services de renseignement déposé le 14 mai 2013 p. 66.

Pour répondre aux évolutions des techniques d'investigations et aux enjeux de protection des libertés publiques, les cadres légaux et les plates-formes dédiées aux interceptions comme au recueil de données techniques de communications doivent être unifiés pour aboutir à un dispositif interministériel, entièrement placé sous l'autorité du Premier ministre et le contrôle de la CNCIS[1].

Pour les techniques spéciales d'enquête qui seraient ouvertes aux services habilités par le Code de la sécurité intérieure, les modalités de leur accès et les conditions de leur contrôle pourraient reprendre les procédures et les règles développées depuis la loi du 10 juillet 1991 en matière d'interception et de recueil des données techniques de communications. Ces nouvelles compétences exigeront des moyens humains, techniques et financiers accrus, notamment avec le recrutement d'ingénieurs et techniciens spécialisés dans les technologies de communications électroniques, pour garantir un suivi complet et efficient.

Les prérogatives de la Délégation parlementaire au renseignement (DPR) sont susceptibles d'être renforcées par la loi relative à la programmation militaire pour les années 2014 à 2019 portant diverses dispositions concernant la défense et la sécurité nationale (LPM).

Il est prévu d'étendre le champ des documents financiers ou stratégiques auxquels la DPR peut avoir accès de même que celui des auditions qu'elle peut pratiquer. Elle devrait absorber, en tant que formation spécialisée, la commission de vérification des fonds spéciaux, prévue par l'article 154 de la loi de finances pour 2002.

Au-delà de ses compétences en matière d'information et de suivi, la DPR se verrait désormais confier l'exclusivité, en matière de renseignement, des pouvoirs de contrôle et d'évaluation de l'action du Gouvernement dévolus au Parlement par l'article 24 de la Constitution.

Jusqu'à cette réforme, la délégation pouvait entendre le Premier ministre, les ministres, le secrétaire général de la défense et la sécurité nationale et les directeurs des services de renseignement. La LPM permettra l'audition du coordonnateur national du renseignement et du directeur de l'Académie du renseignement, ainsi que celle, après accord des ministres dont ils relèvent, des directeurs d'administration centrale ayant à connaître des activités des services spécialisés de renseignement. Il prévoit également l'audition des présidents de la CCSDN et de la CNCIS.

Le renforcement des prérogatives de la DPR s'inscrit dans un contrôle de responsabilité portant sur l'ensemble de l'action des services. Il ne porte pas sur le contrôle de la légalité et de la proportionnalité

---

1) Voir sur ce point le chapitre 3 « Jurisprudence et actualités parlementaires » de la 3ème partie « Études et documents ».

des mesures mises en œuvre, exercé notamment par la CNCIS. Il s'agit donc d'un contrôle complémentaire par rapport à celui conduit par la Commission, et notamment par les deux parlementaires qui la composent, ceux-ci étant, au demeurant, très souvent membres de la DPR.

Même si des amendements d'origine parlementaire ont permis d'infléchir le projet initial de loi relatif à la programmation militaire pour les années 2014 à 2019, celui-ci ne constitue pas la réforme que la CNCIS appelle de ses vœux sur la protection des communications électroniques, et dont les idées-force sont évoquées plus haut.

Cet indispensable travail législatif doit être mené dans les meilleurs délais. Forte de son expertise unique, issue des contrôles effectués comme des avis rendus depuis plus de vingt ans, la CNCIS, qui doit être consultée sur tous les projets liés à ses domaines de compétence [1], prendra toute sa part dans les travaux d'élaboration de cette législation.

La déclassification de données en rapport avec les interceptions de sécurité

Dans la continuité des questions évoquées dans le rapport public de l'an dernier [2], l'actualité de l'année 2012-2013 fonde quelques développements sur la protection dont fait l'objet la mise en œuvre des interceptions de sécurité et sur les hypothèses où cette classification peut être levée.

Le législateur, en 1991, a décidé de maintenir la protection attachée aux dispositifs d'interceptions de sécurité au niveau « secret-défense » [3]. Cette classification est justifiée par le niveau de sensibilité des sujets que couvrent les cinq motifs légaux pour lesquels ces mesures peuvent être ordonnées, par la nécessité de protéger les actions ainsi que les moyens humains et techniques des services habilités, mais aussi par l'indispensable confidentialité, allant au-delà de la présomption d'innocence, qui doit entourer l'identité des cibles des interceptions, qui ne sont pas, au stade administratif, mises en cause pour la commission d'infractions caractérisées.

---

1) L'article 13 de la loi du 10 juillet 1991 (devenu l'article L. 243-1 du Code de la sécurité intérieure), a toujours fondé la saisine de la CNCIS sur tout projet législatif ou réglementaire la concernant ou portant sur les sujets relevant de sa compétence. Bien que le texte soit général et ne contienne pas de dispositions impératives, il a toujours été observé que, par cet article, le législateur a chargé la Commission de veiller au respect des dispositions portant sur les interceptions de sécurité ou le recueil de données techniques de communications. À ce titre, tout projet normatif portant sur son domaine de compétence doit être soumis à son examen.
2) Rapport 2011-2012 p. 40-45.
3) Article L. 243-4 du Code de la sécurité intérieure.

Par conséquent, la protection dont bénéficient les données issues des interceptions de sécurité au titre du secret de la défense nationale ne les rend accessibles à l'autorité judiciaire que dans le cadre de la procédure de déclassification prévue par le Titre 1er du Livre III du Code de la défense, notamment de son article L. 2312-4.

Article L. 2312-4 du Code de la défense : Une juridiction française dans le cadre d'une procédure engagée devant elle peut demander la déclassification et la communication d'informations, protégées au titre du secret de la défense nationale, à l'autorité administrative en charge de la classification.
Cette demande est motivée.
L'autorité administrative saisit sans délai la Commission consultative du secret de la défense nationale.

Les matières traitées dans le cadre des interceptions de sécurité, qui ont, comme le montrent les chiffres exposés dans le chapitre III de ce rapport d'activité, très majoritairement vocation à être « judiciarisées », peuvent donner lieu à des demandes de déclassification.

Parfois, les interceptions de sécurité permettent de constater la commission d'infractions et deviennent le fondement d'une dénonciation à l'autorité judiciaire du crime ou délit, en vertu de l'article 40 alinéa 2 du Code de procédure pénale.

Article 40 alinéa 2 du Code de procédure pénale : Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs.

La CNCIS, à l'instar des différents services habilités qui mettent en œuvre les mesures de surveillance, doit appliquer ces dispositions d'ordre public, sans compromettre le « secret-défense ».

La procédure, pour les services concernés, consiste à faire parvenir au procureur de la République une dénonciation écrite comportant des informations démarquées, qui conduiront le magistrat à faire une demande de déclassification à l'autorité administrative compétente, afin d'identifier les pièces qui peuvent intéresser la justice et solliciter la levée de la protection qui s'attache à elles. Cette hypothèse est explicitement prévue par le législateur de 1991 à l'article L. 242-8 du Code de la sécurité intérieure.

Article L. 242-8 du Code de la sécurité intérieure : Sans préjudice de l'application du deuxième alinéa de l'article 40 du Code de procédure pénale, les renseignements recueillis ne peuvent servir à d'autres fins que celles mentionnées à l'article L. 241-2 [c'est-à-dire « rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous »].

Le Premier ministre, comme la CNCIS, ont ainsi été sollicités par des magistrats chargés de recueillir des éléments utiles à la manifestation de la vérité, et ce quel que soit leur degré de protection. À ce titre, la CNCIS est la seule autorité non ministérielle à avoir saisi la CCSDN en vue de recueillir son avis sur l'éventuelle déclassification de documents sollicités par l'autorité judiciaire[1].

Ainsi, en 2013 le Premier ministre et la CNCIS ont reçu une requête aux fins de déclassification émanant d'un juge d'instruction au tribunal de grande instance de Brive-la-Gaillarde, chargé d'une information judiciaire des chefs « d'atteinte au secret des correspondances émises par voie électronique, d'atteinte au secret ou de suppression de correspondance par dépositaire de l'autorité publique et d'atteinte à l'intimité de la vie privée par captation ou transmission des paroles d'une personne ».

La demande portait sur les documents susceptibles d'être produits et détenus dans le cadre d'une autorisation d'interception et de son exploitation.

Conformément à la procédure prévue par les articles L. 2312-1 et suivants du Code de la défense, la CNCIS a saisi la CCSDN le 5 avril 2013.

Cette AAI a rendu un avis favorable à la déclassification le 16 mai 2013 (publié au *Journal officiel* du 31 mai 2013 et reproduit ci-dessous).

1) *Cf.* rapport 2010-2012 de la CCSDN p. 23 et rapport 2011-2012 de la CNCIS p. 40-45.

JORF n°0124 du 31 mai 2013 page texte n° 98

AVIS

Avis n° 2013-11 du 16 mai 2013

NOR : CSDX1312569V

La Commission consultative du secret de la défense nationale, régulièrement convoquée et constituée, en ayant délibéré,

Vu le Code de la défense, notamment ses articles L. 2312-1 à L. 2312-8 ;

Vu la lettre de saisine de M. le président de la Commission nationale de contrôle des interceptions de sécurité en date du 5 avril 2013 à la suite d'une requête en déclassification en date du 21 février 2013 émanant de Mme Cécile LASFARGUES, juge d'instruction au tribunal de grande instance de Brive-la-Gaillarde, chargée d'une information judiciaire des chefs « d'atteinte au secret des correspondances émises par voie électronique, d'atteinte au secret ou de suppression de correspondance par dépositaire de l'autorité publique et d'atteinte à l'intimité de la vie privée par captation ou transmission des paroles d'une personne ».

Émet un avis favorable à la déclassification et à la communication des deux documents suivants :

– fiche CNCIS/SD. 16236-3 (1 page) ;

– note CNCIS/SD. 16236-2 (4 pages) à l'exception de la phrase de la page 3 commençant par les mots : « l'avis rendu au titre de », du paragraphe de la page 3 commençant par les mots : « Ces mentions » et des deux premiers paragraphes du 4 de la page 4. À l'exception des mentions à caractère interne ou technique dont la protection paraîtra nécessaire à la Commission nationale de contrôle des interceptions de sécurité.

Fait à Paris, le 16 mai 2013

Pour la Commission consultative du secret de la défense nationale :

La présidente, E. Ratte

Par décision du 29 mai 2013, l'assemblée plénière de la CNCIS a procédé à la déclassification de l'intégralité des documents sollicités par le magistrat instructeur. Elle a fait connaître sa décision par un communiqué de presse diffusé le 31 mai 2013.

Chapitre III

Le contrôle des interceptions de sécurité (Titre IV du Livre II du Code de la sécurité intérieure)

Le contrôle des autorisations

Il s'agit ici de décrire la nature et la portée du contrôle opéré par la CNCIS sur les demandes d'interceptions dont elle est saisie. La mission confiée par le législateur est celle d'un contrôle de la légalité. La Commission n'a pas de compétence pour juger de l'opportunité pour un service de choisir ce moyen d'investigation à tel ou tel moment de la conduite de son enquête, ni pour porter une appréciation sur la manière dont les enquêteurs exploiteront les renseignements obtenus. La vérification de la légalité ne se limite pas pour autant à un contrôle formel. Elle porte aussi sur les éléments de procédure et de fond des dossiers d'interceptions.

Ce contrôle intervient en amont de l'autorisation d'interception, sous la forme d'un avis qui est donné au moment de la présentation et de la transmission au GIC des demandes des services habilités validées par le ministre de tutelle. La décision d'autorisation relève du pouvoir exclusif du Premier ministre ou de ses délégués (article L. 242-1 du Code de la sécurité intérieure).

Le contrôle de la Commission s'exerce aussi après cette décision, et ce durant toute l'exploitation de l'interception. Il peut entraîner l'adoption de recommandations d'avertissement ou d'interruption.

Le contrôle en amont

La mission première de la CNCIS est la vérification de la légalité des autorisations d'interceptions. Elle se traduit par un contrôle systématique et exhaustif de l'ensemble des demandes tant au stade initial qu'à celui de l'éventuel renouvellement de l'interception.

La loi nº 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques avait prévu un contrôle *a posteriori*. Toutefois, dès les premiers mois de son fonctionnement, la Commission a instauré, avec l'accord du Premier ministre, la pratique du contrôle préalable à la décision d'autorisation, allant ainsi au-delà de la lettre de l'article L. 243-8 du Code de la sécurité intérieure (ancien article 14 de la loi du 10 juillet 1991).

Ce contrôle *a priori* renforce les modalités de la protection de la correspondance privée. Il constitue une garantie importante en ce que l'avis de la Commission portant sur la légalité et sur la protection du secret des correspondances intervient avant la décision et la mise en œuvre de la mesure d'interception.

Depuis l'instauration de cette procédure d'avis *a priori*, les avis défavorables ont été dans leur grande majorité suivis par l'autorité de décision. En ce sens, cette pratique est plus efficace du point de vue de la protection des libertés publiques que la recommandation prévue par la loi et adressée après la notification de la mise en place d'une interception. Dans ce dernier cas, l'atteinte au secret des correspondances, disproportionnée ou inadaptée, est effective, même si elle est de courte durée, l'interception étant stoppée rapidement après sa mise en œuvre et sa notification à la Commission.

En outre, cette pratique permet un dialogue utile avec les services demandeurs et une meilleure prise en compte par ceux-ci, dès le stade préparatoire, des préconisations de la Commission pour garantir le respect de la loi et l'équilibre entre la défense des intérêts fondamentaux de la Nation et la protection du secret des correspondances. Ce dialogue est enrichi et facilité par le travail de centralisation et d'intermédiation effectué par le GIC.

Cette pratique de l'avis *a priori* a été étendue, par décision de la Commission du 25 mars 2003, aux interceptions demandées en urgence absolue. Elle a été confirmée le 18 février 2008 par une directive du Premier ministre, qui a qualifié ce contrôle *a priori* de « pratique la mieux à même de répondre à l'objectif de protection efficace des libertés poursuivi par le législateur ».

Du fait de cet avis *a priori*, que la demande intervienne selon la procédure « normale » ou en « urgence absolue », les dispositions de l'article L. 243-8 alinéas 1 à 3 du Code de la sécurité intérieure n'ont logiquement plus trouvé à s'appliquer au stade de l'autorisation de l'interception de sécurité.

Elles prévoient en effet que « la décision motivée du Premier ministre mentionnée à l'article L. 242-1 est communiquée dans un délai de 48 heures au plus tard au président de la CNCIS.

Si celui-ci estime que la légalité de cette décision au regard des dispositions du présent titre n'est pas certaine, il réunit la Commission, qui statue dans les sept jours suivant la réception par son président de la communication mentionnée au premier alinéa.

Au cas où la Commission estime qu'une interception de sécurité a été autorisée en méconnaissance des dispositions du présent titre, elle adresse au Premier ministre une recommandation tendant à ce que cette interception soit interrompue ».

La procédure de l'article L. 243-8 conserve néanmoins sa pleine effectivité en ce qui concerne les interceptions déjà en cours et dont la Commission recommande au Premier ministre de décider de les interrompre, ou préconise directement aux services cette interruption.

La Commission sollicite que cette pratique adoptée et reconnue par tous comme une meilleure garantie en termes de droits pour les personnes et d'efficacité soit explicitement prévue par la loi, et ce par ajout d'un alinéa à l'article L. 243-8.

Le contrôle formel des demandes d'interception et le respect des contingents

L'activité de contrôle de chacun des projets d'interception comporte en premier lieu un aspect formel, qui consiste à vérifier que les signataires des demandes d'autorisation ont bien été habilités par les ministres compétents. Devant l'augmentation des demandes urgentes et afin de diminuer les délais de traitement, sur proposition de la Commission, la loi n° 2006-64 du 23 janvier 2006 a introduit à l'article 4 de la loi du 10 juillet 1991 (désormais l'article L. 241-2 du Code de la sécurité intérieure) une disposition autorisant chaque ministre, à l'instar du Premier ministre, à déléguer de façon permanente sa signature à deux personnes.

Les contingents d'interceptions simultanées ne doivent pas être confondus avec le nombre total d'interceptions (demandes initiales et renouvellements) réalisées annuellement au profit des trois ministères concernés : Intérieur, Défense et Budget. Dans son souci de conserver un caractère exceptionnel aux interceptions de sécurité, le législateur de 1991 a en effet opté pour une limitation sous forme d'un encours

maximum, protecteur des libertés publiques (article L. 242-2 du Code de la sécurité intérieure).

Ce système, mis en place par la décision du 28 mars 1960 du Premier ministre Michel Debré, résultait à l'époque de contraintes techniques (capacité maximale d'enregistrement sur des magnétophones à bandes ou à cassettes et capacité d'exploitation par le GIC). Il a été confirmé en 1991 dans le but d'« inciter les services concernés à supprimer le plus rapidement possible les interceptions devenues inutiles, avant de pouvoir procéder à de nouvelles écoutes » (CNCIS, 3e rapport - 1994, p. 16).

L'exigence du respect de ce plafond n'est donc plus la conséquence de contraintes techniques mais un aspect du caractère « exceptionnel » que doit conserver l'atteinte au secret des correspondances de nos concitoyens. Le contingentement participe à l'encadrement de la mise en œuvre des interceptions et demeure un facteur de protection des libertés publiques.

En pratique, il implique que le nombre d'interceptions actives doive à tout moment respecter un plafond fixé par ministère en vertu d'une décision du Premier ministre. La répartition interne entre services est du ressort de chaque ministère et conduit à ce que le nombre des interceptions à un instant donné soit toujours inférieur au contingent. Les services doivent en effet se réserver la possibilité de répondre en permanence à des circonstances inattendues ou à des besoins nouveaux.

L'augmentation constante du parc de vecteurs de communications électroniques (téléphone fixe, mobile, fax, Internet) a conduit à des relèvements progressifs du contingent (50 % depuis l'origine), qu'il faut rapprocher de l'augmentation exponentielle du nombre d'utilisateurs des outils de communication. À titre d'illustration, le nombre d'abonnés à des services mobiles en France est ainsi passé de 280 000 en 1994 à 73,7 millions au 31 mars 2013 soit un taux de développement dans la population (hexagone et outre-mer) de 112,4 %. Par ailleurs, 51 milliards de SMS ont été échangés au cours du premier trimestre 2013, soit presque 250 SMS émis par mois et par abonné (source Autorité de régulation des communications électroniques et des postes [ARCEP]).

Cette comparaison entre, d'une part, l'évolution des outils de communication et leur emploi, et, d'autre part, l'augmentation limitée des contingents d'interceptions depuis 1991, témoigne du respect constant de la volonté du législateur de conserver aux mesures d'ingérence des pouvoirs publics dans la correspondance privée, leur caractère exceptionnel.

Tableau récapitulatif de l'évolution des contingents d'interceptions prévus par l'article L. 242-2 du Code de la sécurité intérieure

	Initial (1991-1996)	1997	2003	Juin 2005	2009
Ministère de la Défense	232	330	400	450	285
Ministère de l'Intérieur	928	1 190	1 190	1 290	1 455
Ministère du Budget	20	20	80	100	100
Total	1 180	1 540	1 670	1 840	1 840

NB : cette modification de la ventilation des contingents d'interceptions attribués à chaque ministère tient compte de l'intégration, depuis 2009, du sous-contingent de la gendarmerie nationale au sein du contingent du ministère de l'Intérieur.

L'année 2012 a été marquée par le quatrième exercice de traitement des interceptions par référence non plus aux « lignes téléphoniques » mais à l'objectif visé par la mesure. Il s'agissait pour la Commission de souligner que les garanties et les droits prévus par la loi du 10 juillet 1991 sont attachés à la personne et non à ses moyens de communications. La protection est homogène et unique pour la personne et ce, quel que soit l'outil de communication électronique employé. Elle permet de garantir l'exploitation légale de l'interception à l'égard d'une seule personne et non d'une pluralité d'individus qui emploieraient le même outil de communication.

Cette référence, à la « cible » devrait permettre de ne pas envisager une augmentation de ce contingent à brève et moyenne échéance, ce qui paraît conforme au respect du caractère exceptionnel que doit conserver cette mesure d'investigation particulièrement attentatoire aux libertés.

Néanmoins, à la lumière des récents travaux consacrés à l'avenir du renseignement, comme le rapport de la mission parlementaire sur l'évaluation du cadre juridique applicable aux services de renseignement déposé le 14 mai 2013[1] et le rapport de la commission d'enquête sur le fonctionnement des services de renseignement français dans le suivi et la surveillance des mouvements radicaux armés déposé le 24 mai 2013[2], et des attentes formulées par les services notamment lors des visites de contrôle opérées par la CNCIS, la question d'une augmentation des « quotas » attribués à certains ministères se pose de nouveau.

Les services utilisateurs ont pu exprimer le souhait d'une augmentation de leur contingent pour faire face à des menaces nouvelles et croissantes d'atteintes aux intérêts fondamentaux de la Nation. Les cas presque inexistants de l'emploi de la totalité du contingent général

1) rapport cité p. 21 et 22
2) rapport cité p. 49 et 50

méritent d'être soulignés dans cette réflexion sur son relèvement, outre la question des capacités d'exploitation des services habilités.

En tous les cas, dans l'avis qu'elle serait amenée à rendre, la CNCIS prendrait en considération les besoins nouveaux des services tout en veillant au respect du caractère exceptionnel que doit conserver l'interception de sécurité, mesure d'investigation particulièrement attentatoire aux libertés.

Contrôle de la motivation et justification de la demande d'interception de sécurité

Le premier et unique objectif des interceptions de sécurité est, comme leur nom l'indique, la protection de la sécurité de la Nation et de ses intérêts fondamentaux.

Les motifs prévus par la loi du 10 juillet 1991, repris à l'article L. 241-2 du Code de la sécurité intérieure, sont directement inspirés du Livre IV du Code pénal qui incrimine les atteintes à ces intérêts fondamentaux. Les cinq motifs légaux de 1991 ne font que décliner les différents aspects de la sécurité de la Nation, mais la référence précise à ceux-ci permet une appréciation plus pertinente du fondement des demandes.

Ces motifs sont : la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de l'article L. 212-1 du Code de la sécurité intérieure sur les groupes de combat et les milices privées.

Les services demandeurs doivent donc faire référence de manière explicite à l'un de ces motifs légaux. Ils doivent en outre justifier leur demande par des explications circonstanciées qui permettront à la Commission d'apprécier l'articulation du fait au droit. À cet effet, la présentation des éléments de fait doit être certes synthétique mais non stéréotypée. Elle doit être sincère et consistante pour permettre à chaque autorité, ministres demandeurs, Commission et Premier ministre, de juger de la pertinence de leur adéquation au motif légal. Ce point, ainsi que les critères d'appréciation des motivations, seront repris dans la partie du rapport consacrée aux « avis et préconisations de la Commission ».

Le cadre des demandes servant à la rédaction des demandes par les différents services habilités a été revu en 2006, en 2008, et à nouveau en 2009. Il est appelé à évoluer prochainement, la CNCIS ayant le souci constant d'améliorer la lisibilité comme la compréhension de ses avis. L'objectif est de constituer des trames toujours plus claires et précises pour tendre, à partir de modèles, à une présentation complète, gage d'une plus grande facilité pour les services rédacteurs et d'une plus grande efficacité dans le traitement de la demande par les autorités de consultation et de décision. Ces imprimés permettent un contrôle

toujours plus efficient de la Commission, qui est très attentive au caractère exhaustif des mentions.

Ces trames normalisées ne constituent pas un cadre restreint. En tant que de besoin, les services peuvent communiquer tout élément qui leur paraît utile à l'appui de leur demande, en présentant spontanément des informations complémentaires indispensables à une appréhension juste et complète de la situation.

Le contrôle opéré par la Commission s'attache d'une part à une identification aussi précise que possible des cibles, d'autre part aux informations recueillies sur leur activité socioprofessionnelle : il convient en effet de porter une attention particulière aux professions ou activités jugées sensibles en raison du rôle qu'elles jouent dans une société démocratique.

Il importe aussi de s'assurer que le motif légal invoqué ne dissimule pas d'autres préoccupations. Il est nécessaire de rappeler que l'interception doit être sollicitée exclusivement pour les faits décrits dans la demande et non pour une raison autre, qui ne relèverait d'aucun motif légal. Ceci sera également développé dans la partie du rapport consacrée aux « avis et préconisations de la Commission ».

La Commission formule toutes les observations qu'elle juge utiles sur la pertinence du motif invoqué, procédant le cas échéant à des propositions de requalification, afin de substituer au motif initialement visé, un autre des cinq motifs légaux qui paraît plus adapté.

Elle s'assure que la demande respecte le principe de proportionnalité entre le but recherché et la mesure sollicitée. La gravité du risque pour la sécurité des personnes – physiques comme morales – ou pour la sécurité collective, doit être à la mesure de l'atteinte à la vie privée que constitue la surveillance de la correspondance par voie de communications électroniques, et la justifier pleinement.

La recherche de cette proportionnalité peut se traduire *ab initio* ou lors du renouvellement par une restriction, au cas par cas, de la durée de la mesure dont le maximum légal est de quatre mois. Une différenciation des délais a ainsi été instaurée par voie jurisprudentielle : deux mois pour une cible non encore totalement identifiée, un mois en cas de risque de récidive d'une infraction criminelle déjà commise, ou encore délai *ad hoc*, calé sur un événement prévu à une date déterminée.

Des instructions peuvent être données pour exclure des transcriptions (appelées « productions ») certains aspects privés des conversations ou des questions n'entrant pas dans le champ des motifs légaux. Des avis favorables subordonnent l'exploitation des interceptions à certains objectifs ou fixent les orientations exclusives qui paraissent devoir être retenues pour garantir une exploitation des communications conforme aux dispositions légales. La Commission et l'autorité de décision

sollicitent régulièrement des bilans circonstanciés avant d'autoriser une nouvelle prolongation dans le cas d'une interception déjà renouvelée.

La Commission veille par ailleurs à ce que soit respecté le principe de subsidiarité. Par conséquent, lors de ses vérifications, elle s'assure que le but recherché ne puisse être rempli que par ce moyen et non par d'autres investigations plus classiques (enquête de terrain, d'environnement, mise en place de forces de l'ordre, etc.).

Depuis sa création, la CNCIS porte une attention particulière à la protection des libertés de conscience et d'expression. Ainsi maintient-elle que le prosélytisme religieux, comme l'expression d'opinions extrêmes, dès lors qu'elles ne tombent pas sous le coup de la loi, ne justifient pas, en tant que tels, une demande d'interception, s'ils ne comportent aucune menace immédiate pour l'ordre public républicain, matérialisée par exemple par un appel ou un encouragement à la violence. De même, elle veille à ce que les interceptions, en ce qu'elles sont parfois concomitantes d'actions sur le terrain, ne portent pas atteinte à la liberté de manifestation.

D'une manière générale, et quel que soit le motif, l'implication personnelle de la cible dans des agissements attentatoires à notre sécurité doit être au moins présumée.

Dans le cadre de son contrôle *a priori*, la Commission dispose d'un moyen d'investigation auquel elle recourt plus souvent depuis quelques années. Elle a la possibilité de demander au service concerné les éléments d'information complémentaires qui lui sont nécessaires pour fonder son avis. Elle peut, en effet, à réception de ces renseignements additionnels, formuler des observations ou rendre un avis défavorable.

Le Premier ministre – ou son délégué – peut, dans les mêmes conditions, solliciter des éléments d'informations supplémentaires. Cette demande suspend, jusqu'à réception des compléments sollicités, la décision d'autorisation ou de renouvellement. Cette requête ou celle initiée par le Premier ministre ou son délégué constitue un sursis à statuer en ce que l'avis préalable doit être recueilli avant l'autorisation et la mise en place d'une interception.

En effet, les renseignements complémentaires sont destinés à compléter, éclairer ou préciser les demandes d'interceptions de sécurité initiales ou de renouvellement. Ces éléments d'information supplémentaires fondent l'avis de la Commission et la décision du Premier ministre, au même titre que les renseignements figurant dans la demande du service.

Par avis no 7/2012 du 29 mai 2012, la Commission a rappelé que les demandes de renseignements complémentaires formulées par la CNCIS ne constituent pas un avis, mais relèvent des mesures d'investigations prévues aux articles L. 243-8 à L. 243-10 du Code de la sécurité intérieure. Ces demandes emportent donc sursis à statuer durant le délai

de réponse du service demandeur et du traitement de cette réponse par la Commission.

Elles peuvent intervenir tant dans le cadre des procédures ordinaires que des urgences absolues, pour les demandes initiales comme pour les renouvellements. La Commission a également rappelé que « les autorisations délivrées par le Premier ministre ou son délégué après une demande de renseignements complémentaires et sans disposer de l'avis de la Commission relèvent des décisions visées par l'article L. 243-8 alinéas 2 et 3 [du Code de la sécurité intérieure]. À ce titre, elles font l'objet d'une recommandation adressée au Premier ministre et au ministre ayant proposé l'interception ».

Données chiffrées et commentaires

• Évolutions 2011-2012

6 145 interceptions de sécurité ont été sollicitées en 2012 (4 022 interceptions initiales et 2 123 renouvellements). Pour mémoire, 6 396 interceptions de sécurité avaient été sollicitées en 2011 (4 156 interceptions initiales et 2 240 renouvellements). Ces chiffres démontrent une légère diminution du nombre d'interceptions pratiquées (- 4 %), sans remettre en cause la stabilité observée depuis plusieurs années.

S'agissant des interceptions initiales, 622 de ces 4 022 demandes ont été présentées selon la procédure dite d'urgence absolue (541 en 2011) soit 15,5 % de ces demandes, ce qui démontre une augmentation légère par rapport à l'année précédente (13 % en 2011). Les neuf premiers mois d'exercice de l'année 2013 montrent une augmentation plus importante du recours à la procédure de l'urgence dont le nombre, au 30 septembre dernier, a atteint celui de l'année écoulée. L'ancrage dans le temps et l'accélération des crises au niveau international, comme leur prolongement prévisible sur le territoire national, constituent sans doute une première cause de ce recours plus important à la procédure de l'urgence. D'autres facteurs, actuellement examinés avec les services demandeurs, seront développés au terme de l'exercice 2013, dans le prochain rapport d'activité de la CNCIS.

L'objectif d'un traitement par la Commission de ce type de demande dans un délai inférieur à une heure a toujours été atteint. Le respect de cette contrainte de performance que s'est fixée l'autorité administrative indépendante nécessite, dans le cadre de l'avis *a priori* donné par la CNCIS, la mise en œuvre d'une permanence 24h/24, tout au long de l'année, qui peut d'une certaine manière être comparée à celle qui est assurée par chaque parquet près les tribunaux de grande instance.

Au final, si l'on impute à ce chiffre global les cinquante avis défavorables donnés par la Commission lors des demandes initiales et des demandes de renouvellement, tous suivis par le Premier ministre, ce

sont donc 6 095 interceptions de sécurité qui ont effectivement été pratiquées au cours de l'année 2012 (6 341 en 2011).

Pour ce qui concerne les « motifs légaux » au stade des autorisations initiales, la prévention de la criminalité et de la délinquance organisées reste le premier motif des demandes initiales avec 66 %, suivie de la prévention du terrorisme avec 19 % et de la sécurité nationale avec 15 %.

Concernant les renouvellements accordés, on note que la sécurité nationale occupe la première place avec 42 % suivie de la prévention du terrorisme à 29 % et de la criminalité organisée à 27 %. Ces pourcentages de renouvellement rendent compte, de fait, du travail des services en rapport avec certains motifs légaux qui supposent une inscription des investigations dans la durée.

La part beaucoup moins importante du motif de la criminalité organisée dans les demandes de renouvellement, alors qu'il constitue plus de la moitié des demandes initiales, est l'application des principes fixés par la loi et repris par le Conseil constitutionnel sur la primauté de l'autorité judiciaire.

Si les projets d'infractions sont confirmés, dans ce cas, les tentatives et la commission des infractions relèvent de la compétence exclusive de l'autorité judiciaire. Comme tous les agents de l'État, les services exploitant des interceptions et constatant à cette occasion l'existence d'infractions doivent en rendre compte à l'autorité judiciaire en application de l'article 40 du Code de procédure pénale. Le pouvoir judiciaire est la seule autorité en charge de l'opportunité et de la conduite des poursuites pénales. Dans ce cas, de nouvelles interceptions peuvent être réalisées. Elles relèvent des dispositions du Code de procédure pénale et sont conduites dans le cadre d'une enquête ou d'une ouverture d'information judiciaire.

Si l'interception de sécurité et les autres investigations ne permettent pas de confirmer les présomptions d'implication personnelle et directe de l'objectif dans des projets de commission d'infractions visées par l'article 706-73 du Code de procédure pénale, il n'y a pas lieu, comme pour les autres motifs, de poursuivre les écoutes.

Le taux de clôture des demandes d'interception pour ouverture d'une procédure judiciaire traduit le respect de ces principes constitutionnels. Il témoigne aussi de l'intérêt de ce dispositif de prévention et de police administrative qui permet d'exclure des hypothèses d'enquête et de stopper les mesures d'investigation avant toute phase judiciaire. Il ouvre aussi la possibilité, en cas de confirmation des soupçons quant à des projets d'infractions, de poursuivre par l'ouverture d'une procédure judiciaire avant la commission des faits, ce qui est particulièrement essentiel dans le cadre de la prévention des attentats terroristes.

Le total cumulé des demandes initiales et des renouvellements ayant été autorisés confirme que la prévention de la criminalité et de la

délinquance organisées se détache nettement avec 52 % des requêtes, suivie de la sécurité nationale à 24 % et puis la prévention du terrorisme à 23 %. Ces trois motifs représentent quasiment 99 % du total des demandes.

• Observations

La Commission a poursuivi sa démarche de dialogue avec les services demandeurs. Cette volonté de privilégier les échanges constructifs s'est traduite par une nette augmentation des réunions bilatérales avec ces mêmes services, tant au niveau central que déconcentré.

Elle s'est également matérialisée, au stade de l'examen des demandes, par des avis ne répondant pas à une logique purement binaire (avis favorable ou défavorable). De fait, le nombre d'observations a encore crû, passant de 3 126 en 2011 dont 114 demandes de renseignements complémentaires et 634 limitations de la durée d'interception sollicitée, à 3 767 en 2012 dont 172 demandes de renseignements complémentaires et 771 limitations de la durée d'interception. Les avis défavorables, comptabilisés dans les observations se sont élevés à 50, 28 concernant les demandes initiales (dont une portant sur une procédure d'urgence absolue) et 22 pour les demandes de renouvellement. À ce chiffre des avis défavorables « bruts », il convient d'ajouter deux techniques d'observation déjà répertoriées dans le rapport d'activité 2008 qui peuvent s'apparenter à « l'avis défavorable » :
– la recommandation adressée au Premier ministre visant à l'interruption de l'interception en cours d'exploitation qui résulte de l'examen exhaustif des « productions » (transcriptions) opérées à partir d'une interception. Il y a été fait recours à quatorze reprises en 2012 (contre sept en 2010 et une en 2011). Elles ont été suivies par le Premier ministre ;
– la « préconisation d'interruption » adressée par la Commission au service utilisateur en cours d'exploitation. Elle résulte du même examen des productions et procède d'un dialogue constructif mené directement avec les services utilisateurs à stopper l'exploitation d'interceptions, qui sont susceptibles de présenter des difficultés par rapport aux dispositions légales ou qui s'éloignent du cadre de l'autorisation délivrée par le Premier ministre ou son délégué. Trente-huit préconisations ont été faites en 2012 par la Commission, toutes suivies par les services titulaires de l'autorisation d'interception.

De fait, si l'on additionne avis défavorables, recommandations d'interruption adressées au Premier ministre et « préconisations d'interruption » adressées directement aux services utilisateurs, le nombre de cas où une interception de sécurité n'a pas été réalisée ou poursuivie, conformément au positionnement de la Commission s'établit pour l'année 2012 à 102.

Le contrôle en aval

Le contrôle en amont des demandes, aussi minutieux et exhaustif soit-il, ne saurait suffire. Le contrôle des « productions » est, en aval, le moyen privilégié pour s'assurer non seulement de la bonne adéquation de la demande au motif légal invoqué, mais aussi de l'intérêt réel présenté par l'interception, au regard des critères de proportionnalité et de subsidiarité.

Ce « contrôle continu » inauguré en 2005 s'effectue de manière aléatoire ou ciblée. Il permet ainsi à la Commission de rendre des avis plus éclairés au stade du renouvellement de l'interception s'il est demandé par le service, et, le cas échéant, d'effectuer, en cours d'exploitation d'une interception, une recommandation tendant à l'interruption de celle-ci.

Ainsi, les « productions » de 561 interceptions en 2012 ont été examinées plus spécifiquement par la Commission. Ce nombre, identique à celui de 2010 (560), est légèrement inférieur à celui de 2011 (619) et résulte mécaniquement de la diminution du nombre total d'interceptions sollicitées en 2012.

La pratique de la « recommandation d'avertissement » décrite dans le rapport 2008 a également été poursuivie : il s'agit d'une lettre annonçant au Premier ministre qu'une recommandation d'interruption de l'écoute pourrait lui être envoyée à bref délai si l'incertitude sur l'adéquation entre le motif invoqué et la réalité des propos échangés devait se poursuivre. Une recommandation a été adressée au Premier ministre au cours de l'année 2012. Elle a entraîné des rappels de la part du délégué du Premier ministre, adressés au service exploitant, qui a tiré les conséquences des difficultés soulevées par la Commission en demandant à son niveau la suppression des interceptions concernées.

Un tel « avertissement » sortant le dossier litigieux de son anonymat administratif, permet au Premier ministre d'interroger le service concerné sur une base concrète, et renforce ainsi, au niveau politique, le dialogue déjà amorcé par la Commission avec les services habilités, au cours de ces dernières années.

Enfin, la Commission procède, en séance plénière, à des auditions de directeurs ou responsables techniques des services de renseignement dans des dossiers où le recueil d'informations complémentaires et le suivi des productions ne suffisent pas à l'éclairer suffisamment avant qu'elle rende ses avis ou formule ses préconisations.

Avec 6 145 interceptions accordées en 2012 par le Premier ministre, rapportées à un nombre de vecteurs de communications électroniques pourtant en constante augmentation, les interceptions de sécurité sont demeurées, comme les années précédentes, la mesure d'exception voulue par la loi.

Tableaux annexes

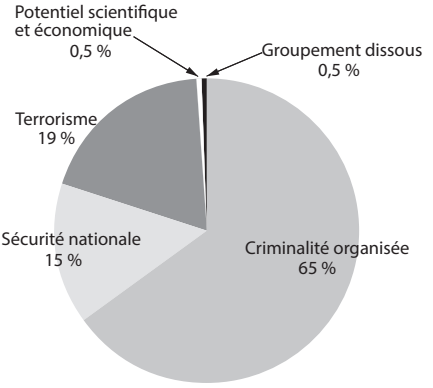
Les demandes initiales d'interceptions

État des demandes initiales d'interceptions (2011 et 2012)

	Demandes initiales		Dont urgence absolue		Accordées	
	2011	2012	2011	2012	2011	2012
Total	4156	4022	541	622	4125	3994

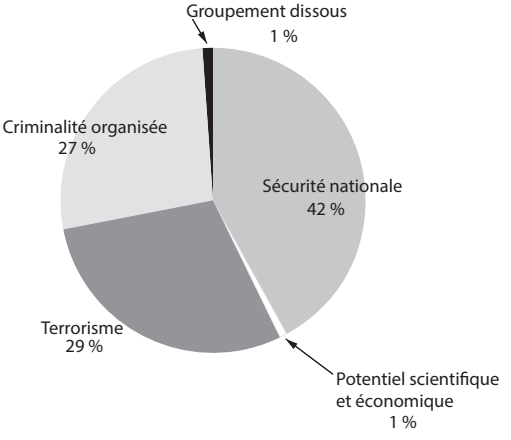
Demandes initiales

Répartition des motifs 2012



Les renouvellements d'interceptions

Total des renouvellements demandés : 2123
Répartition des motifs des renouvellements accordés en 2012



Activité globale : demandes initiales et renouvellements

Répartition des demandes entre interceptions et renouvellements d'interceptions

Demandes initiales circuit normal		Demandes initiales en urgence absolue		Demandes de renouvellement	
2011	2012	2011	2012	2011	2012
3615	3400	541	622	2240	2123

2012

Demandes initiales : 65,4 %. 15 % d'entre elles ont été sollicitées selon la procédure de l'urgence absolue.

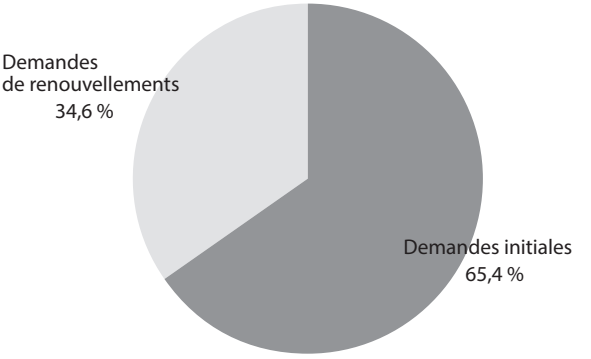
Demandes de renouvellements : 34,6 %.

Demandes d'interceptions : tableau récapitulatif global sur sept ans 2006 à 2012

	2006	2007	2008	2009	2010	2011	2012
Demandes initiales d'interceptions	4203	4215	4330	3176	3776	4156	4022
Dont « urgences absolues »	714	964	1095	497	522	541	622
Demandes de renouvellements	1825	1850	1605	1941	2234	2240	2123
Total	6028	6065	5935	5117	6010	6396	6145

Répartitions des motifs d'interceptions de sécurité accordées :

Cumul des demandes initiales et demandes de renouvellements accordés



Répartition entre interceptions et renouvellements accordés

Interceptions accordées en 2012

Interceptions initiales	Renouvellements	Total
3994	2101	6095

Le contrôle de l'exécution

Celui-ci porte sur trois domaines :
– l'enregistrement, la transcription et la durée des interceptions ;
– les visites des centres déconcentrés, des services départementaux et régionaux ainsi que des échelons nationaux qui procèdent aux demandes et à l'exploitation des interceptions de sécurité ;
– l'instruction des réclamations des particuliers et les éventuelles dénonciations à l'autorité judiciaire.

Enregistrement, transcription et destruction

La mise en place en 2002 d'un effacement automatisé de l'enregistrement au plus tard à l'expiration du délai de dix jours, prévu par l'article L. 242-6 du Code de la sécurité intérieure, s'est traduite par un gain de temps appréciable pour les agents chargés de l'exploitation. Cette évolution ne dispense cependant pas de l'accomplissement des formalités prévues par le deuxième alinéa de ce même article : « Il est dressé procès-verbal de cette opération [de destruction des enregistrements à l'expiration d'un délai de dix jours]. » En application de cette disposition, en début d'année civile, le directeur du GIC atteste de la conformité logicielle du parc informatique de tous les établissements placés sous son autorité.

Les transcriptions doivent être détruites, conformément à l'article L. 242-7 du Code de la sécurité intérieure, dès que leur conservation n'est plus « indispensable » à la réalisation des fins mentionnées à l'article L. 241-2, même si cet article L. 242-7 n'édicte pas de délai. Le GIC à la faveur d'une instruction permanente a, conformément aux prescriptions de l'IGI 1300/SGDN/SSD du 30 novembre 2011, imposé aux services destinataires finaux des productions, d'attester auprès de lui de la destruction effective de ces dernières, dès lors que leur conservation ne présentait plus d'utilité pour l'exécution de la mission poursuivie.

Le contrôle du GIC

Service du Premier ministre, consacré comme tel après trente et une années d'existence par le décret n° 2002-497 du 12 avril 2002 (CNCIS, 11e rapport, 2002, p. 50) et actuellement dirigé par un officier général, le GIC est l'élément clef du dispositif des interceptions de sécurité. Il en assure la centralisation conformément à l'article L. 242-1 alinéa 2 du Code de la sécurité intérieure (« Le Premier ministre organise la centralisation de l'exécution des interceptions autorisées »).

Cette centralisation des moyens d'écoute, placés sous l'autorité du Premier ministre et confiés à un service technique neutre, qui n'est pas en charge de l'exploitation du renseignement et des enquêtes, a été jugée par le législateur comme une garantie fondamentale dans la protection

des libertés publiques en ce qu'elle offre une séparation claire et solide entre l'emploi des moyens et les services de renseignement, entre le demandeur et l'autorité de décision. Au regard de ses attributions, la Commission a toujours réaffirmé l'importance de cette organisation et de ce principe comme une garantie essentielle au bon fonctionnement démocratique des institutions en charge de ces outils de renseignement et d'investigation.

Ce service s'adapte en permanence aux avancées technologiques incessantes dans le domaine des communications électroniques qui constituent chaque fois autant de défis à relever (citons en l'espace d'une décennie, la téléphonie mobile, le SMS, le mail, l'Internet, le dégroupage et la multiplication des opérateurs).

Conformément à une recommandation prise par la Commission en 1996, le GIC a entrepris dès 1997 la mise en place de centres locaux de regroupement des interceptions, sortes de « GIC déconcentrés » répondant aux normes de sûreté souhaitées par la Commission au regard de la protection des personnes mise en cause et des personnels des services chargés de l'exploitation de ces renseignements.

Cette phase est à ce jour achevée. Le maillage du territoire en antennes secondaires se poursuit désormais pour s'adapter aux évolutions des menaces, au redéploiement des services ainsi qu'aux réformes territoriales et des administrations. Après la nécessaire étape de la structuration centralisée voulue par le législateur et le gouvernement, il a été donné aux services enquêteurs la proximité attendue pour une plus grande efficacité de leurs investigations, en créant des centres d'exploitation dans le ressort territorial de leurs missions. Les moyens d'interception et leur contrôle demeurent centralisés. Ce redéploiement des centres d'exploitation, au plus près des utilisateurs, est une garantie d'efficience sur le plan opérationnel, tout en préservant les garanties d'un système centralisé placé sous l'autorité du Premier ministre, contrôlé à la fois par un service du Premier ministre et une AAI.

Enfin, le GIC répond à toute demande d'information de la Commission, qu'il assiste avec célérité et efficacité.

Les visites des centres déconcentrés et des services locaux

En dépit d'une situation de sous-effectif durant le premier trimestre 2012, la CNCIS a poursuivi les visites inopinées ou programmées des services utilisateurs d'interceptions.

Lors de ces visites, les contrôles portent à la fois sur la sécurisation des locaux, les interceptions en cours, l'examen des relevés d'interception et d'enregistrement (article L. 242-4 du Code de la sécurité intérieure) et des procès-verbaux de destruction des enregistrements et des transcriptions (articles L. 242-5 et L. 242-7 du Code de la sécurité intérieure).

Ces déplacements peuvent être effectués par les membres de la Commission eux-mêmes, le délégué général ou le chargé de mission.

Au total, sous une forme ou sous une autre, dix-huit visites de centres d'exploitation et d'échelons centraux ont été effectuées cette année. À chacune de ces visites, les représentants de la CNCIS dressent un inventaire des pratiques et procédures mises en œuvre par les services pour l'application du Code de la sécurité intérieure, apportent les informations et éclaircissements utiles, notamment sur le rôle et les avis de la CNCIS, recueillent les observations des personnels rencontrés sur les matériels et logiciels mis à leur disposition et s'informent des problématiques locales et nationales se rapportant aux motifs légaux des interceptions.

Réclamations de particuliers et dénonciation à l'autorité judiciaire

Les saisines de la CNCIS par les particuliers

En 2012, cinquante-deux particuliers ont saisi par écrit la CNCIS. Une minorité des courriers concernait des demandes de renseignements sur la législation. La majorité, constituée de réclamations, a donné lieu au contrôle systématique auquel il est procédé lorsque le demandeur justifie d'un intérêt direct et personnel à interroger la Commission sur la légalité d'une éventuelle interception administrative.

Il convient de préciser que les agents de la Commission ont traité un chiffre d'appels téléphoniques bien supérieur à celui des saisines par courrier. Ces contacts préalables ont le plus souvent permis de prévenir des courriers ultérieurs inappropriés lorsqu'il s'agit d'appels malveillants, de problèmes relevant de la saisine de l'autorité judiciaire (soupçons d'écoutes illégales à caractère privé) ou enfin de dysfonctionnements techniques classiques. Les requérants ont pu ainsi être réorientés vers les services compétents ou les autorités en charge de ces questions.

S'agissant des courriers adressés à la CNCIS, il leur est immédiatement donné suite et il est notifié au requérant, conformément à l'article L. 243-11 du Code de la sécurité intérieure, que la Commission a « procédé aux vérifications nécessaires ». On relève à ce propos dans les débats parlementaires précédant l'adoption de la loi du 10 juillet 1991 que « l'imprécision de cette formule reprise à l'identique de l'article 39 de la loi du 6 janvier 1978 [loi informatique et libertés] et reprise à l'article 41 de cette même loi, telle que modifiée par la loi du 6 août 2004 peut sembler insatisfaisante mais il est difficile, notamment au regard des prescriptions de l'article 26 de la loi du 10 juillet 1991 modifiée par la loi du 9 juillet 2004, d'aller plus loin dans la transparence. En effet, à l'occasion de son contrôle, la Commission peut découvrir les situations suivantes :
– existence d'une interception ordonnée par l'autorité judiciaire ;

– existence d'une interception de sécurité décidée et exécutée dans le respect des dispositions légales ;
– existence d'une interception de sécurité autorisée en violation de la loi ;
– existence d'une interception "sauvage", pratiquée par une personne privée en violation de l'article L241-1 du code de la sécurité intérieure.
– absence de toute interception.

On comprendra aisément au vu de ces différentes hypothèses que la CNCIS n'a d'autre possibilité que d'adresser la même notification à l'auteur d'une réclamation, quelle que soit la situation révélée par les opérations de contrôle, et que toute autre disposition conduirait, directement ou indirectement, la Commission à divulguer des informations par nature confidentielles » (Assemblée nationale, rapport no 2088 de François Massot, 6 juin 1991).

Faut-il en conclure que toute requête est inutile ? Non, car même si le « secret-défense » interdit toute révélation sur l'existence ou l'inexistence d'une interception de sécurité, la CNCIS dispose de deux moyens d'action lorsqu'elle constate une anomalie :
– le pouvoir d'adresser au Premier ministre une recommandation tendant à faire interrompre une interception qui s'avérerait mal fondée ;
– le pouvoir, qui est aussi un devoir, de dénonciation à l'autorité judiciaire de toute infraction à la loi de 1991 (aujourd'hui Titre IV du Livre II du Code de la sécurité intérieure) qui pourrait être révélée à l'occasion de ce contrôle (*cf. infra*).

Pour être complet signalons que :
– la CADA arguant du secret-défense a émis le 18 décembre 1998 un avis défavorable à la demande de communication d'une copie d'une autorisation du Premier ministre concernant l'interception éventuelle des communications téléphoniques d'un requérant ;
– le Conseil d'État, dans une décision du 28 juillet 2000, a rejeté le recours d'un requérant contre la décision du président de la CNCIS refusant de procéder à une enquête aux fins, non de vérifier si des lignes identifiées avaient fait l'objet d'une interception comme la loi lui en donne le pouvoir, mais si la surveillance policière dont l'intéressé se disait victime trouvait sa source dans l'interception de lignes de ses relations.

Les avis à l'autorité judiciaire prévus à l'article L. 243-11 du Code de la sécurité intérieure

Au cours de l'année 2012, la CNCIS n'a pas eu à user des dispositions du 2e alinéa de l'article L. 243-11 du Code de la sécurité intérieure qui précisent que « conformément au deuxième alinéa de l'article 40 du Code de procédure pénale, la Commission donne avis sans délai au procureur de la République de toute infraction aux dispositions de la présente loi dont elle a pu avoir connaissance à l'occasion du contrôle effectué en application de l'article L. 243-9 ».

Chapitre IV

Le contrôle des opérations portant sur les données techniques de communications

Section 1 - Présentation du dispositif

En matière de police administrative et de prévention des atteintes à la sécurité et aux intérêts fondamentaux de la Nation, le recueil de données techniques de communications repose sur deux cadres légaux. La Commission, assistée des services du Groupement interministériel de contrôle et de ceux de la « personnalité qualifiée » de l'article 6 de la loi du 23 janvier 2006, exerce un strict contrôle sur ces deux modes de réquisitions administratives.

I – Le régime de l'article L. 244-2 du Code de la sécurité intérieure (ex-article 22 de la loi du 10 juillet 1991)

La loi nº 91-646 du 10 juillet 1991 est le premier texte en matière d'exploitation des communications électroniques pour la prévention des atteintes les plus graves à la sécurité nationale et aux intérêts fondamentaux de la Nation. Son article 22 – désormais article L. 244-2 du Code de la sécurité intérieure – constitue la première référence légale aux données techniques de communications.

Ce texte prévoit que les onze services habilités, par le biais du GIC, peuvent « recueillir, auprès des personnes physiques ou morales exploitant des réseaux de communications électroniques ou fournisseurs de services de communications électroniques, les informations ou documents qui leur sont nécessaires, chacun en ce qui le concerne, pour la réalisation et l'exploitation des interceptions autorisées par la loi ». Le GIC, pour satisfaire les demandes, est en relation avec près de soixante-dix opérateurs de réseaux de communications électroniques ou opérateurs virtuels.

Sur ce fondement légal, les demandes d'identification et de données de trafic auprès du GIC sont faites par les services en vue de l'élaboration d'un projet d'interception de sécurité. Ces mesures s'inscrivent dans le cadre de la réalisation visée par la loi, soit l'action de rendre réel et effectif une interception potentielle, ou de l'exclure au terme des résultats de ces investigations préparatoires. S'agissant de mesures moins attentatoires au secret des correspondances, elles constituent ainsi le moyen d'exclure des projets d'interceptions plus intrusives par l'accès qu'elles permettent au contenu des communications.

De même, sur la base de cet article, les prestations annexes, portant sur les communications électroniques de l'objectif visé par l'interception (Fadettes, localisation…), sont transmises par les opérateurs, *via* le GIC, au service exploitant, durant toute la durée de l'écoute. Dans ce cas, les mesures se fondent sur l'exploitation visée explicitement par la loi.

Ce dispositif est mis en œuvre pour tous les motifs légaux de l'article L. 241-2 du Code de la sécurité intérieure (la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, la prévention du terrorisme, de la criminalité et de la délinquance organisées ainsi que de la reconstitution ou du maintien de groupements dissous) et par tous les services, hormis, s'agissant de la prévention du terrorisme, ceux du ministère de l'Intérieur, qui doivent recourir aux dispositions prévues par l'article L. 34-1-1 du Code des postes et des communications électroniques.

Ces données techniques sont recueillies au terme d'une procédure spécifique, organisée conformément aux recommandations de la CNCIS. La Commission a défini une procédure de contrôle reposant sur les principes de la loi du 10 juillet 1991 et adaptée à la nature du recueil des données :
– la centralisation, le traitement et le contrôle *a priori* des demandes des services par le Groupement interministériel de contrôle, relevant du Premier ministre ;
– le contrôle *a posteriori* de ces demandes par la CNCIS, qui a accès à l'ensemble de la procédure, à tout instant ;
– la possibilité pour la Commission, de recourir aux mêmes avis et recommandations que ceux adressés au Premier ministre, dans le cadre des interceptions de sécurité.

II – Le dispositif expérimental de l'article 6 de la loi du 23 janvier 2006 (article L. 34-1-1 du Code des postes et des communications électroniques)

À la suite des attentats de Madrid du 11 mars 2004 et de Londres du 7 juillet 2005, le législateur a autorisé les services de police et de gendarmerie spécialisés dans la prévention du terrorisme à se faire communiquer, sur le fondement d'une réquisition administrative spécifique, certaines données techniques détenues par les opérateurs de communications.

L'article 6 de la loi n° 2006-64 du 23 janvier 2006, relative à la lutte contre le terrorisme et portant diverses dispositions relatives la sécurité et aux contrôles frontaliers, autorise les services du ministère de l'Intérieur, chargés de la prévention du terrorisme, à recueillir, sur simple réquisition, des données techniques afférentes à une communication électronique. Il permet d'avoir accès au « contenant » d'une telle communication sans avoir accès au « contenu » de celle-ci, c'est-à-dire la conversation proprement dite.

Il encadre très strictement cet accès en le limitant au seul motif de la prévention des actes de terrorisme et en fixant limitativement les prestations qui peuvent être obtenues. Il permet notamment le recueil des données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, le recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, des données relatives à la localisation des équipements terminaux utilisés, ainsi que des données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications.

Quoique moins intrusive dans le secret des correspondances, cette mesure porte atteinte à d'autres droits des citoyens, comme le droit à l'intimité de la vie privée et à la liberté d'aller et venir. C'est la raison pour laquelle le législateur a prévu un certain nombre de garanties au respect desquelles la CNCIS est associée pleinement.

Ainsi, la loi du 23 janvier 2006 a adopté un dispositif original en instituant une « personnalité qualifiée » auprès du ministre de l'Intérieur, relevant pour partie de la CNCIS concernant son activité de contrôle de la légalité des demandes des services habilités en matière de prévention du terrorisme. La Commission est en outre chargée du contrôle *a posteriori* de toutes les demandes validées par la « personnalité qualifiée ». La loi n° 2012-1432 du 21 décembre 2012 a décidé de proroger « une dernière fois » [1] l'expérimentation, jusqu'au 31 décembre 2015.

---

1) Le ministre de l'Intérieur a souligné lors des débats devant le Sénat (16 octobre 2012) et l'Assemblée nationale (27 novembre 2012), que cette prolongation du dispositif expérimental était la dernière, l'objectif du gouvernement étant l'unification rapide de ce cadre temporaire avec celui de l'article L. 244-2 du Code de la sécurité intérieure.

Section 2 - Statistiques de l'activité pour l'année 2012

I – Concernant l'article L. 244-2 du Code de la sécurité intérieure

Au cours de l'année 2012, le GIC a traité 197 057 demandes. 190 431 d'entre elles portaient sur des mesures d'identification, ainsi que sur des prestations spécifiques comme l'historique d'un identifiant ou l'identification d'une cellule. 6 626 mesures de détails de trafics ont par ailleurs été examinées. L'ensemble des requêtes satisfaites représente une hausse de 10 % par rapport à l'année 2011 [1].

Il convient de préciser que les services du ministère de l'Intérieur sollicitent par cette procédure des données techniques pour l'ensemble des motifs autres que celui de la prévention du terrorisme. Les services qui dépendent des ministères de la Défense ou du Budget recourent au GIC pour l'ensemble des cinq motifs légaux, y compris en matière de terrorisme, puisqu'ils ne font pas partie des services habilités au titre de l'article 6 de la loi du 23 janvier 2006.

Les demandes se répartissent entre les différents motifs légaux de la façon suivante : 70 % d'entre elles portent sur la sécurité nationale, 21 % ont trait à la prévention de la délinquance et de la criminalité organisées, 7 % concernent la prévention du terrorisme, 4 % sont relatives à la protection du potentiel scientifique et économique et 2 % visent la reconstitution de groupements dissous.

7 % des mesures sont refusées et 10 % d'entre elles font l'objet de renvoi pour renseignements complémentaires avant validation.

II – Concernant l'article 6 de la loi du 23 janvier 2006

Sur les cinq années d'expérimentation (de 2008 à 2012), après une augmentation régulière du nombre de demandes présentées par les services, l'année 2011 avait marqué un spectaculaire retournement de tendance, avec 11 635 demandes de moins que l'année précédente. Cette tendance baissière s'est poursuivie en 2012, mais dans une moindre mesure. En effet, le dernier exercice s'est conclu sur un total de 29 322 demandes présentées, soit 4 759 de moins que l'année précédente. La tendance du premier semestre de l'année 2013 laisse entrevoir une légère remontée du nombre de requêtes.

---

1) En 2011, le GIC avait traité 179 948 demandes de prestations annexes, dont 176 755 portaient sur des mesures d'identification, ainsi que sur des prestations spécifiques comme l'historique d'un identifiant ou l'identification d'une cellule, et 3 193 portaient sur des détails de trafics.

	Demandes présentées	Demandes validées	Demandes renvoyées	Demandes rejetées
2008	38393	34998	3302	93
2009	43559	39070	4459	30
2010	45716	38566	7060	90
2011	34081	31637	2428	16
2012	29322	26563	2736	23
Total sur cinq ans	191071	170834	19985	252

Les demandes validées ne correspondent pas au nombre d'objectifs. Dans la majorité des cas, plusieurs dizaines de demandes concernent en fait une seule personne soupçonnée de menées terroristes. La recherche d'un renseignement va fonder le recours à plusieurs opérateurs de communications électroniques. Des mesures différentes sont sollicitées pour la même personne au fur et à mesure de l'évolution des investigations et de leur résultat.

La typologie des mesures sollicitées par les services est identique quelle que soit la période d'exercice, soit près de 75 % de demandes d'identification d'abonnés. Ces mesures sont moins intrusives que les demandes portant sur les données de trafic qui représentent près de 25 % des dossiers traitées.

La diminution du recours au dispositif de l'article 6 par les services en charge de la prévention du terrorisme, déjà évoquée dans les rapports d'activité des années 2010 et 2011, s'est accrue en 2012 avec une baisse de 27,48 % des demandes présentées, et, corrélativement une diminution de 26,35 % des demandes validées.

Dans son précédent rapport, la CNCIS avait tenté de dresser l'inventaire des principaux facteurs susceptibles d'expliquer cette baisse, alors que la France se trouve depuis quelques années dans un contexte de menaces terroristes élevées. Les constatations et les analyses faites sur la période 2012 confirment les principales hypothèses évoquées à l'époque, notamment celle d'une utilisation plus ciblée des mesures au regard de leurs conditions d'accès et des résultats qu'elles permettent en matière de renseignement.

Sur ce dernier point, il appert que les mesures dont les résultats confirment les hypothèses d'enquête aboutissent dans la quasi-totalité des cas à des demandes d'interception de sécurité dont une partie de la motivation repose sur les renseignements issus du recueil de données techniques de communication.

Ces constats confirment l'intérêt d'un cadre légal unique et général régissant les interceptions de communication et le recueil de leurs données, qu'appelle de ses vœux la Commission depuis plusieurs années.

En 2012, les services de la Direction centrale du Renseignement intérieur (DCRI), de la Direction du Renseignement de la préfecture

de police (DRPP) et de l'Unité de coordination de la lutte antiterroriste (UCLAT) ont été à l'origine de 97,4 % des 29 322 requêtes présentées dans le cadre du dispositif de l'article 6, ce qui constitue une donnée stable par rapport à l'année précédente.

Concernant les services et les unités à vocation judiciaire, qui emploient ce dispositif au titre du renseignement et de la prévention du terrorisme, 767 demandes ont été formulées, essentiellement par la Direction centrale de la Police judiciaire (DCPJ) (49,8 %) et la Direction générale de la Gendarmerie nationale (DGGN) (45,6 %).

Les mesures sollicitées visent les moyens de communication électronique suivants

	2008	2009	2010	2011	2012
Téléphonie fixe	13,81 %	17,96 %	21,02 %	19,58 %	19,84 %
Téléphonie mobile	82,10 %	70,03 %	68,11 %	66,38 %	67,23 %
Internet	4,09 %	12,01 %	10,87 %	14,04 %	12,93 %

Ces chiffres permettent un triple constat :
– la téléphonie mobile reste la technologie qui motive le plus grand nombre de demandes ;
– le nombre des requêtes concernant la téléphonie fixe reste stable depuis trois ans autour de 20 % ;
– les prestations Internet, après une hausse en 2011, se stabilisent autour de 13 %.

Les données provisoires de l'activité en 2013 paraissent confirmer ces tendances.

Section 3 - Étendue et modalités du contrôle exercé par la CNCIS

Les demandes faites par les services doivent comporter des renseignements précis sur l'objectif et le moyen de communication visé. Elles doivent être motivées. Ces éléments sont indispensables tant dans la phase de validation que du contrôle *a posteriori*.

Les requêtes fondées sur l'article 6 de la loi du 23 janvier 2006 sont validées préalablement par la « personnalité qualifiée » placée auprès du ministre de l'Intérieur et nommée par la CNCIS pour une durée de trois ans renouvelable, ou par l'un de ses adjoints nommés dans les mêmes conditions. Elles doivent être sollicitées par des « agents individuellement désignés et dûment habilités ».

Les demandes relevant de l'article L. 244-2 du Code la sécurité intérieure sont validées par les personnels de permanence et de direction du GIC.

La loi a conféré à la CNCIS la responsabilité de contrôler *a posteriori* l'activité de ces deux entités et de saisir le ministre de l'Intérieur ou le Premier ministre d'une « recommandation » quand elle « constate un manquement aux règles […] ou une atteinte aux droits et libertés ».

La Commission a adressé une recommandation au ministre de l'Intérieur en 2012, portant sur trois dossiers distincts en rappelant la vocation exclusivement préventive et de renseignement du dispositif de l'article 6. Par décision n° 2005-532 DC du 19 janvier 2006, le Conseil constitutionnel a réaffirmé ce principe à propos de ce dispositif instauré par la loi du 23 janvier 2006, en rappelant la primauté de l'autorité judiciaire.

S'agissant du contrôle de légalité *a priori* et de la validation, la « personnalité qualifiée » a privilégié le recours régulier aux demandes de renseignements complémentaires avant validation ou refus. Le nombre de refus est ainsi resté à un niveau extrêmement bas (0,08 % en 2012).

Les motifs principaux de refus et de recommandations, au titre de l'article 6 de la loi du 23 janvier 2006, sont liés à des demandes relatives à des faits déjà commis et/ou faisant l'objet d'enquêtes judiciaires, à des demandes concernant des cibles dont la situation pénale au regard du Code de procédure pénale impose de prendre d'autres mesures et à des requêtes relatives à des faits insusceptibles en l'état de constituer des menées terroristes.

Les motifs essentiels de rejet des demandes au titre de l'article L. 244-2 du Code de la sécurité intérieure portent sur l'insuffisance des présomptions d'implication personnelle et directe de la personne visée par les demandes, le non-respect des principes de proportionnalité et/ou de subsidiarité, la contradiction entre les faits exposés et le motif légal de la demande et l'absence de précisions sur les projets d'atteintes aux intérêts fondamentaux de la Nation et à la sécurité.

La CNCIS a renforcé sa mission de contrôle en poursuivant les réunions avec la « personnalité qualifiée » et le GIC pour assurer une unicité de traitement des demandes portant sur les mesures référentielles de recueil de données techniques de communications, quel que soit le cadre légal, s'agissant d'investigations et d'atteintes au secret des correspondances identiques.

La Commission a apporté des précisions sur le contrôle gradué des requêtes en fonction du caractère plus ou moins intrusif de la prestation sollicitée au regard des libertés individuelles.

Elle a surtout développé le recours au « droit de suite », aux fins de connaître, dans un nombre plus important de dossiers les résultats des

mesures ainsi validées. La Commission dispose ainsi d'éléments lui permettant d'apprécier la pertinence des demandes au regard des principes de proportionnalité et de subsidiarité.

Section 4 - Réflexions sur le projet d'unification des cadres légaux du recueil de données techniques de communications en matière de police administrative

Éléments de droit comparé

Le rapport 2011-2012 avait déjà abordé les travaux conduits par la CNCIS avec un certain nombre d'organismes en charge du contrôle des interceptions des communications électroniques d'États étrangers (Allemagne, Belgique, Liban, Bulgarie, Roumanie, Italie, notamment). Ces réflexions se sont poursuivies à la lumière des échanges intervenus durant l'année 2012-2013, en particulier avec le Canada, ou encore la Turquie.

Il ressort de ces analyses comparées que certaines législations prévoient un régime unique pour les demandes d'interceptions et celles portant sur des données techniques (Allemagne). D'autres ont des régimes comparables à celui du système français, avec des dispositions plus explicites et plus précises sur les mesures qui peuvent être sollicitées par les services de renseignement, ainsi que sur la nature des menaces ou des atteintes fondant ces actions administratives préventives (Belgique). D'autres encore ne disposent pas de législation sur les données techniques de communications. Certains pays s'intéressent depuis quelques années aux dispositifs d'interception et de surveillance générale, aléatoire, par balayage ou exhaustif, des communications électroniques. Ils retiennent alors un contrôle *a posteriori* portant sur l'exploitation du renseignement technique.

Dans tous les cas, les délégations étrangères rencontrées et les organismes étrangers consultés ont montré un intérêt particulier pour les dispositions françaises, notamment sur le régime différencié de protection et d'autorisation, qui varie selon la nature et l'importance de l'atteinte portée au secret des correspondances et à la vie privée.

Éléments de l'évaluation faite par la CNCIS

La CNCIS conduit en permanence, en sa qualité d'organe de contrôle de la légalité chargé de la protection du secret des correspondances privées par voie électronique, une évaluation des cadres légaux

de recueil de données techniques de communications, et ce depuis la mise en œuvre effective des dispositifs en 2007.

En 2012, dans la perspective du renouvellement envisagé du cadre expérimental de l'article 6 de la loi du 23 janvier 2006, la CNCIS avait procédé à un bilan complet et argumenté de ce dispositif, que le président a pu exposer lors d'auditions devant les Commissions des lois du Sénat puis de l'Assemblée nationale en octobre 2012 dans le cadre des travaux préparatoires de la loi n° 2012-1432 du 21 décembre 2012, qui a prorogé une dernière fois, pour trois ans l'expérience conduite.

Cette évaluation a aussi été menée au regard des évolutions du dispositif du GIC sur les interceptions de sécurité et le recueil des données techniques de communications, pour tous les motifs prévus par la loi du 10 juillet 1991, y compris la prévention du terrorisme lorsqu'elle est mise en œuvre par les services habilités des ministères de la Défense et des Finances.

Cette analyse s'est appuyée sur les avis et les recommandations antérieurs de la CNCIS, en particulier son avis délivré en formation plénière le 14 septembre 2005, qui rappelait que « le recueil de données techniques générées par les communications électroniques ou par Internet, appelées prestations annexes, fait l'objet de l'article 22 de la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques [...]. Le droit positif relatif au recueil de données techniques prévoit un régime unique pour l'ensemble des motifs légaux et autorise l'atteinte au secret des correspondances, justifiée par l'intérêt supérieur de la sécurité nationale et la protection de la vie des populations. Dès lors, l'adoption d'une procédure spécifique et d'un dispositif spécial pour le seul motif de la prévention du terrorisme ne paraît pas pertinente. Ce régime est même contraire à la volonté du législateur de centraliser les outils relatifs aux interceptions des communications électroniques et de les placer sous une autorité de décision distincte des services utilisateurs et des ministères demandeurs ».

Dans le cadre des auditions devant les Commissions des lois des deux chambres parlementaires en octobre 2012, la CNCIS a rappelé que la juxtaposition de deux régimes qui offrent les mêmes prestations, mais selon des modalités de fonctionnement juridiques et techniques différentes, était source de confusion pour les services utilisateurs, d'erreurs dans le choix du cadre procédural, voire dans certains cas de tentatives pour utiliser successivement l'un et l'autre des cadres en cas de refus d'une des autorités décisionnaires.

Elle a également souligné que les menaces sont de plus en plus transversales et que les enquêteurs travaillent sur des objectifs « multicartes » (criminalité organisée, atteintes à la sécurité nationale ou terrorisme, par exemple). Dès lors, la coexistence de deux dispositifs cloisonnés peut entraîner des difficultés dans le travail d'investigation et de renseignement, ainsi que dans la mise en œuvre d'un régime unique

et cohérent de protection des correspondances privées par voie des communications électroniques.

Elle a rappelé que le rattachement au ministère de l'Intérieur du dispositif UCLAT de recueil de données techniques de communications pour la prévention du terrorisme, effectué par les services de ce même ministère, déroge aux principes fondamentaux du système mis en œuvre depuis la loi du 10 juillet 1991 [1].

La Commission a noté avec satisfaction que son analyse avait été très largement reprise lors des débats parlementaires ayant conduit à l'adoption de la loi nº 2012-1432 du 21 décembre 2012, tant par le ministre de l'Intérieur que par les principaux orateurs des différents groupes. L'unification des dispositifs est désormais un objectif consensuel.

De plus, la convergence « technique » est, de fait, imminente, puisque la plate-forme de l'UCLAT, qui permettait depuis 2007 le recueil des données techniques de communications sollicitées dans le cadre de l'article 6 de la loi du 23 janvier 2006 ne pourra pas prendre en compte les nouveaux modes de traitement entre les services de l'État et les opérateurs de communications électroniques, et ce d'ici quelques mois. Dans ces conditions, les perspectives les plus probables sont celles d'un traitement des requêtes adressées à l'UCLAT par le GIC, préfigurant en cela le futur régime unique.

L'objectif étant fixé et les conditions techniques largement définies et bientôt effectives, il reste à préciser selon quelles modalités l'unification devra être mise en place d'ici le 31 décembre 2015.

La CNCIS rappelle qu'un régime unique peut être défini dans le cadre de la loi du 10 juillet 1991, aujourd'hui Titre IV du Livre II du Code de la sécurité intérieure. En effet, ce texte garantit l'équilibre entre, d'une part, les impératifs de sécurité et de préservation des intérêts fondamentaux de la Nation, et, d'autre part, la protection des droits et des libertés individuelles, en consacrant la séparation entre les services habilités relevant de ministères demandeurs et l'autorité de décision. Le Premier ministre dispose d'un service technique autonome (le GIC) et se place sous le contrôle de légalité d'une AAI.

Il offre un cadre légal pertinent et fondé juridiquement pour le recueil des données techniques de communications en matière de prévention du terrorisme. Ce motif est explicitement prévu par la loi pour autoriser à déroger, à titre exceptionnel, au respect du secret des

---

1) Ces principes sont : une autorité de décision distincte des services habilités et des ministères demandeurs garantissant le recours à titre exceptionnel à ces investigations, et ce par une analyse partagée et contradictoire ; une autorité de décision disposant d'un outil centralisé de mise en œuvre et de contrôle technique des mesures, structure ne relevant pas des services utilisateurs ; une autorité de contrôle, dont l'indépendance statutaire renforce les garanties de protection des libertés publiques définies par le législateur.

correspondances privées par voie électronique. Il est mis en œuvre pour les interceptions de sécurité des services habilités et pour le recueil de données techniques des services ne relevant du champ d'application de la loi du 23 janvier 2006.

En outre, face aux menaces et aux objectifs précités, la réponse paraît plus pertinente en matière de sécurité juridique si elle consiste dans un dispositif global, cohérent, sécurisé, parfaitement contrôlé, et prenant en compte l'ensemble des motifs légaux.

Il faut désormais que ce projet soit concrétisé par une modification législative. La CNCIS souhaite que cette réforme, indispensable et urgente, intervienne le plus rapidement possible.

Section 5 - Élaboration d'un cadre légal pour la géolocalisation en temps réel

La géolocalisation est une méthode permettant d'obtenir et de transmettre, au besoin en temps réel, la position géographique d'une personne ou d'un objet. Elle peut passer par la localisation d'un équipement permettant des échanges par la voie des communications électroniques.

En l'état actuel de la législation, la géolocalisation en temps réel n'est prévue par aucun texte et ce contrairement à ce qui existe dans d'autres pays (par exemple l'Allemagne). Cette mesure ne fait pas partie des données techniques de communications conservées et traitées par les opérateurs de communications électroniques en application de l'article L. 34-1 du Code des postes et des communications électroniques. Elle nécessite en effet, en l'état de la technologie, l'envoi de requêtes volontaires récurrentes obligeant le terminal de l'utilisateur à se localiser.

La CEDH s'est prononcée sur cette question de droit, à l'occasion d'une affaire où la géolocalisation en temps réel a été utilisée en matière de terrorisme. Elle a estimé que l'usage de cette mesure consistait à recueillir des données sur la vie privée de la personne visée et qu'elle devait donc être prévue par la loi, conforme au principe de subsidiarité, proportionnée au but poursuivi, limitée dans sa durée, et soumise à un contrôle [1].

Le projet de loi relatif à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale déposé au Sénat le 2 août 2013 a, pour la première

---

1) Voir notamment l'arrêt *Uzun c. Allemagne* du 2 septembre 2010 et, s'agissant de la jurisprudence nationale, les arrêts très récents de la chambre criminelle de la Cour de cassation du 22 octobre 2013, cités dans le chapitre 3 de la 3ème partie du présent rapport.

fois, prévu, dans son article 13, de donner un fondement légal explicite à cette mesure.

La CNCIS relève avec le plus grand intérêt que le travail législatif qu'elle appelle de ses vœux depuis plusieurs années est désormais entamé dans le but d'intégrer cette mesure particulière de recueil de données techniques de communications, en ce qu'elle permet d'accéder à des informations sur la vie privée non prévues en l'état du droit et selon des procédés non spécifiés dans les obligations des opérateurs de communications électroniques, en matière de réquisitions des services de l'État.

Néanmoins, la Commission déplore de n'avoir pas été consultée lors des travaux préparatoires de la LPM. En effet, l'article 13 de la loi du 10 juillet 1991 (devenu l'article L. 243-1 du Code de la sécurité intérieure), a toujours fondé la saisine de la CNCIS sur tout projet législatif ou réglementaire la concernant ou portant sur les sujets relevant de sa compétence. Bien que le texte soit général et ne contienne pas de dispositions impératives, il a toujours été observé que, par cet article, le législateur a chargé la Commission de veiller au respect des dispositions portant sur les interceptions de sécurité ou le recueil de données techniques de communications. À ce titre, tout projet normatif portant sur son domaine de compétence doit être soumis à son examen.

Au cours des précédentes modifications de la loi du 10 juillet 1991 ou dans le cadre de l'élaboration de textes nouveaux comme la loi du 23 janvier 2006, la Commission a été en mesure de fournir un avis destiné à éclairer le travail d'élaboration de la norme, à tous les stades de la procédure législative ou réglementaire, en qualité d'autorité administrative chargée du contrôle de la mise en œuvre des interceptions et du recueil de données en matière de communications électroniques.

Or, il n'apparaissait pas pour la Commission que le projet initial de modification réponde parfaitement aux exigences de la situation et puisse constituer une base juridique pérenne. L'article L. 34-1-1 du Code des postes et des communications électroniques porte, comme évoqué précédemment, sur un dispositif provisoire, adopté à titre expérimental, dont la fin est prévue le 31 décembre 2015, et ce après une seconde prorogation par la loi du 21 décembre 2012 relative à la sécurité et la lutte contre le terrorisme.

Ainsi les demandes relevant de l'article L. 34-1-1 du Code des postes et des communications électroniques seront prises en compte par la plateforme du GIC, laquelle relève, à la base, de l'article L. 244-2 du Code de la sécurité intérieure. Dès lors, il paraissait singulier que l'outil qui devra réaliser les mesures de géolocalisation en temps réel soit celui qui relève d'un code entièrement muet sur cette mesure. De plus, l'article L. 34-1-1 ne vise que la prévention du terrorisme et ne peut être mis en œuvre que pour les services du ministère de l'Intérieur, habilités au titre de l'article 6 de la loi du 23 janvier 2006.

Par ailleurs, le Code des postes et des communications électroniques traite des questions relatives aux obligations légales des opérateurs de communications électroniques. Il ne porte pas spécifiquement sur les mesures qui peuvent être prises par les services de renseignement ou à vocation judiciaire pour les motifs prévus par la loi et les infractions qui autorisent les actions intrusives des pouvoirs publics dans les communications électroniques privées. En ce sens, la CNCIS considère que l'article L. 34-1-1 modifié ne répond pas parfaitement aux critères retenus par la CEDH.

Or, en ce qu'elle apporte des éléments extrêmement utiles à l'avancement des enquêtes menées pour la recherche de renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous, il paraît au contraire important d'inscrire cette mesure dans le cadre pérenne du Titre IV du Livre II du Code de la sécurité intérieure issu de la loi n° 91-646 du 10 juillet 1991, afin de permettre une mise en œuvre de cette technique d'enquête par un dispositif interministériel, placé sous l'autorité du Premier ministre, ouvert aux trois ministères habilités à effectuer des interceptions de sécurité et des recueils administratifs de données techniques de communications (Défense, Intérieur et Budget), pour les cinq motifs précités, le tout sous le contrôle d'une autorité administrative indépendante : la CNCIS.

Pour ces raisons, la Commission renouvelle son souhait d'une modification non pas de l'article L. 34-1-1 du Code des postes et des communications électroniques mais de l'article L. 244-2 du Code de la sécurité intérieure (ancien article 22 de la loi du 10 juillet 1991), dans la mesure où ce texte vise l'ensemble des motifs légaux pour lesquels des interceptions de sécurité et des recueils de données techniques de communications peuvent être autorisés.

Cette modification constituerait en outre une première étape vers l'unification des procédures de recueils de données techniques préconisée par la CNCIS, reprise dans le Livre blanc sur la défense et la sécurité nationale rendu public le 29 avril 2013, puis dans le rapport de la mission parlementaire sur l'évaluation du cadre juridique applicable aux services de renseignement déposé le 14 mai 2013, et à nouveau dans le rapport de la commission d'enquête sur le fonctionnement des services de renseignement français dans le suivi et la surveillance des mouvements radicaux armés déposé le 24 mai 2013, ainsi que par le ministre de l'Intérieur à l'occasion des débats parlementaires sur le vote de la loi relative à la sécurité et la lutte contre le terrorisme du 21 décembre 2012[1].

---

1) Voir le chapitre 3 « Jurisprudence et actualités parlementaires » de la 3ème partie du présent rapport sur les débats actuellement en cours au Parlement dans le cadre du projet de loi de programmation militaire pour les années 2014 à 2019.

Chapitre V

Le contrôle portant sur les matériels d'interception

En vertu des articles R. 226-1 à R. 226-12 du Code pénal, le Premier ministre est compétent pour accorder les autorisations de fabrication, d'importation, d'exposition, d'offre, de location, de vente, d'acquisition ou de détention de matériels permettant de porter atteinte à l'intimité de la vie privée ou au secret des correspondances.

Ces autorisations interviennent après avis d'une commission consultative dite « R 226 » dont la CNCIS est membre permanent.

Depuis le décret 97-757 du 10 juillet 1997, la CNCIS a toujours soutenu qu'un contrôle plus efficace des interceptions de sécurité devait porter non seulement sur les demandes d'interception et leur exploitation par les services de l'État, mais également sur les matériels et les équipements acquis, importés, détenus et utilisés par des sociétés privées et les services de l'État, qui comportent des possibilités d'interceptions des communications électroniques.

La structure de cette commission consultative a été modifiée à la faveur de deux décrets publiés durant l'année 2009. Ainsi, le décret n° 2009-834 du 7 juillet 2009 puis le décret n° 2009-1657 du 24 décembre 2009 ont confié la présidence de cette commission au directeur général de l'ANSSI, lui-même rattaché au secrétaire général de la défense et de la sécurité nationale. Cette mutation structurelle n'a en revanche emporté aucune modification dans l'économie juridique du dispositif existant.

Le régime de contrôle, issu de l'arrêté du 29 juillet 2004 aujourd'hui abrogé et remplacé par l'arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du Code pénal, participe d'une évolution de l'appréhension de ce secteur d'activité sensible

par la puissance publique[1]. Il traduit une vision libérale quant à la mise sur le marché d'appareils dont la liste initiale a été réduite, vision assortie d'une logique de vigilance quant à l'utilisation finale de ces appareils[2].

Si les règles de commercialisation ont été allégées par rapport au dispositif réglementaire antérieur à 2004, cette facilitation de l'accès au marché n'a pas induit une inflexion dans la qualification du caractère « sensible » de ce type de matériel par les pouvoirs publics.

Ainsi, le décret 2005-1739 du 30 décembre 2005 réglementant les relations financières avec l'étranger et portant application de l'article L. 151-3 du Code monétaire et financier (présenté par la doctrine comme aménageant le contrôle des investissements étrangers dans les secteurs stratégiques en France – *Recueil* Dalloz 2006, p. 218) soumet au principe de l'autorisation préalable l'investissement d'un État (intra ou extracommunautaire) portant sur « les matériels conçus pour l'interception des correspondances et la détection à distance des conversations autorisés au titre de l'article 226-3 du Code pénal ».

La commission consultative prévue à l'article R. 226-2 du Code pénal s'est réunie six fois en 2012. Sa composition est la suivante :
– le directeur de l'ANSSI ou son représentant, président ;
– un représentant du ministre de la Justice ;
– un représentant du ministre de l'Intérieur ;
– un représentant du ministre de la Défense ;
– un représentant du ministre chargé des Douanes ;
– un représentant du ministre chargé de l'Industrie ;
– un représentant de la CNCIS ;
– un représentant de l'Agence nationale des fréquences ;
– deux personnalités désignées en raison de leur compétence par le Premier ministre.

En 2012, la commission a connu, comme les années précédentes, une augmentation de son activité, même si elle est de moindre ampleur que l'an passé. Elle a ainsi rendu 970 décisions (contre 558 en 2009, 643 en 2010 et 883 en 2011) ventilées comme suit :
– 642 décisions d'autorisation initiale (428 concernant la commercialisation, 214 l'acquisition d'équipements soumis à autorisation) ;
– 47 décisions de renouvellement d'autorisation ;
– 217 décisions d'ajournement ;
– 17 décisions de radiation ou d'annulation ;
– 38 décisions de refus ou de retrait ;
– 5 décisions de mise en attente ;
– 4 décisions de mise « hors champ » de l'examen pour autorisation.

1) *cf.* rapport 2004, p. 34-38 ; rapport 2005, p. 31-33.
2) *cf.* rapport 2004, p. 38.

L'année 2012 a confirmé la tendance nouvelle observée en 2010 : le nombre de décisions de mise « hors champ » de l'examen de la Commission a continué à nettement diminuer, pour ne finalement concerner que 4 dossiers (contre 53 en 2009, 15 en 2010 et 8 dossiers en 2011).

Cette évolution est vraisemblablement le résultat d'une meilleure connaissance, par les intervenants privés et publics, des dispositions de l'arrêté du 29 juillet 2004, qui portent sur l'exclusion de certains types d'appareils auparavant soumis à autorisation.

La CNCIS est également membre de la commission d'examen des demandes émanant des services de l'État pouvant solliciter une « autorisation de plein droit », conformément aux dispositions de l'article R. 226-9 du Code pénal.

Les administrations concernées sont invitées, selon le régime mis en place en 2001[1], à produire leurs registres et à décrire leurs règles internes de gestion des matériels sensibles. Sans préjudice des autres contrôles qui peuvent être opérés sur pièces et sur place par la commission consultative ou par l'AAI en vertu de ses pouvoirs propres, l'examen de ces demandes permet aux représentants de la CNCIS de s'assurer du respect des règles adoptées en matière d'emploi, ainsi que de l'adéquation des matériels détenus avec les missions confiées à ces services.

Par ailleurs, la loi relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale (LPM) prévoit d'élargir le champ de deux incriminations pénales[2] réprimant les cas de fabrication, de détention ou d'utilisation de matériels pouvant servir à enregistrer des conversations privées, à capter des données informatiques ou à intercepter des correspondances.

L'extension consiste à couvrir non plus seulement les seuls matériels conçus pour commettre des atteintes à la vie privée mais également ceux qui sont de nature à permettre une utilisation à ces fins. Cette modification de la loi implique un réexamen de l'arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du Code pénal.

Si le degré de protection attaché aux travaux de cette commission dite « R 226 » ne permet pas d'en détailler le contenu, la CNCIS rappelle que ses avis au sein de cette structure reposent sur le souci constant de protéger les citoyens contre tout enregistrement à leur insu de communications ou de données qui y sont rattachées, et ce en raison d'un emploi inadapté ou frauduleux des fonctionnalités d'interception et de captation, offertes par certains matériels.

---

1) *cf.* rapport 2001, p. 27.
2) Prévues et réprimées par les articles 226-1 à 226-3 et 226-15 du Code pénal (atteintes à la vie privée et au secret des correspondances).

Deuxième partie

Avis et préconisations de la Commission

Chapitre I

Avis et préconisations de la Commission portant sur les motifs légaux en matière d'interceptions de sécurité et de recueil des données techniques de communications

Le rapport public est le moyen de faire une présentation générale et développée de chacun des motifs retenus par la loi et appliqués par la Commission dans ses avis. Ces critères sont repris intégralement par les autorités qui sont chargées d'autoriser ou non ces mesures de renseignement et de police administrative en matière de communications électroniques.

S'agissant de mesures classifiées « secret défense » ou « confidentiel défense », seuls les principes généraux de la qualification juridique peuvent être exposés dans ce rapport public.

Sécurité nationale

« Sécurité nationale », « sécurité intérieure et extérieure », « sûreté de l'État », « intérêts fondamentaux de la Nation » sont des concepts voisins souvent employés indistinctement. Pour autant, le concept de « sécurité nationale » est apparu comme une nouveauté en 1991 et son usage est spécifique à la loi du 10 juillet 1991.

On relève ainsi dans les travaux parlementaires (rapport de la Commission des lois du Sénat) que « la notion de sécurité nationale est préférée à celle d'atteinte à la sûreté intérieure et extérieure de l'État […]. La sécurité nationale, notion qui n'existe pas en tant que telle dans le droit français est directement empruntée à l'article 8 de la Convention européenne des droits de l'homme. Elle recouvre la défense nationale ainsi que les autres atteintes à la sûreté et à l'autorité de l'État qui figurent au début du Titre 1er du Livre troisième du Code pénal ».

Pour mémoire, on rappellera que l'article 8 § 2 de la CEDH : « Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit (droit au respect de la vie privée et familiale) que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

Les anciens articles 70 à 103 auxquels se référait le législateur en 1991 sont les incriminations visées désormais dans le Livre IV du Code pénal en vigueur 1994 et dénommées « atteintes aux intérêts fondamentaux de la Nation ».

Les intérêts fondamentaux de la Nation constituent depuis 1994 un concept destiné à remplacer celui de sûreté de l'État qui avait lui-même succédé, dans l'ordonnance du 4 juin 1960, à celui de sécurité intérieure et extérieure.

Selon l'article 410-1 du Code pénal : « Les intérêts fondamentaux de la Nation s'entendent au sens du présent titre de son indépendance, de l'intégrité de son territoire, de sa sécurité, de la forme républicaine de ses institutions, de ses moyens de défense et de sa diplomatie, de la sauvegarde de sa population en France et à l'étranger, de l'équilibre de son milieu naturel et de son environnement et des éléments essentiels de son potentiel scientifique et économique et de son patrimoine naturel. »

On notera que la sauvegarde des éléments essentiels du potentiel scientifique et économique constitue un motif d'interception autonome dans la loi de 1991.

Dès l'entrée en vigueur du Nouveau Code pénal en 1994, la CNCIS a estimé que la notion de sécurité nationale devait être définie par référence à ces dispositions pénales (article 410-1 du Code pénal) portant sur les intérêts

fondamentaux de la Nation en intégrant les notions d'intégrité du territoire, de forme républicaine des institutions ou des moyens de la défense.

S'il s'agit là d'un élargissement notable de la notion antérieure de sûreté de l'État, on ne saurait y voir pour autant une extension par assimilation aux atteintes les plus courantes à la sécurité des personnes ou des biens. La Commission a toujours rappelé qu'il ne suffit pas d'invoquer la crainte générale d'un trouble à l'ordre public, comme y expose plus ou moins toute manifestation, pour répondre aux exigences de motivation résultant de la loi. Pour ce faire, il doit être justifié, avec la précision nécessaire, d'une menace particulièrement grave à la sécurité nationale.

Ainsi des demandes motivées par la crainte d'un trouble à l'ordre public ne peuvent fonder le recours à une interception qu'en cas de menace particulièrement grave à la sécurité. Le risque d'attenter à la forme républicaine des institutions ou de déboucher sur un mouvement insurrectionnel est fondamental. Si des manifestations sont susceptibles de dégénérer, le droit de manifester étant constitutionnellement reconnu, il s'agit là, d'un problème d'ordre public et non d'une atteinte à la sécurité nationale. On peut cependant admettre que dans certaines hypothèses, l'ampleur des troubles ou les atteintes aux institutions voulues par leurs auteurs affectant le lieu et le temps des manifestations, la qualité des autorités ou des symboles républicains visés, sont tels que la sécurité nationale peut être menacée.

Les interceptions de sécurité ne sauraient être utilisées comme moyen de pénétrer un milieu syndical ou politique ou de pratiquer la surveillance d'opposants étrangers, si la sécurité de l'État français lui-même n'est pas en cause. S'agissant de la recherche de renseignements, la personne dont il est envisagé d'intercepter les correspondances doit être suspectée d'attenter par ses agissements personnels aux intérêts fondamentaux de la Nation. Si les services de renseignements ont, par nature, une mission de collecte de renseignements qu'ils remplissent en utilisant divers moyens, intrusifs ou non dans le champ des libertés publiques, le recours aux interceptions de sécurité connaît certaines limites. En effet, l'atteinte exceptionnelle à la vie privée qu'autorise la loi ne peut être justifiée même dans ce domaine que par la menace directe ou indirecte, actuelle ou future que la personne écoutée est susceptible de représenter pour la sécurité nationale. En l'absence de menace, et quel que soit l'intérêt que représente la cible comme source de renseignement pour le domaine considéré, l'atteinte à la vie privée serait contraire aux principes de proportionnalité et de subsidiarité.

Enfin, la Commission opère une appréciation *in concreto* de la notion « d'intérêts fondamentaux de la Nation », la notion de sécurité étant appréhendée en un instant donné et dans un contexte géopolitique donné par rapport aux besoins vitaux du pays. Ainsi la Commission considère depuis plusieurs années que la sécurité énergétique fait désormais intégralement partie de la sécurité nationale.

Sauvegarde des éléments essentiels du potentiel scientifique et économique de la Nation

La sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, est, avec la prévention de la reconstitution ou du maintien de groupements dissous, le motif d'interception le plus faible en volume, bien qu'il connaisse quelques développements avec les enjeux en lien avec « l'intelligence économique », la contre-ingérence, ainsi qu'avec les questions d'espionnage industriel et scientifique.

C'est cependant celui qui, lors de la discussion parlementaire de la loi du 10 juillet 1991, a suscité le plus de réserves.

La rédaction initiale n'était d'ailleurs pas celle adoptée. Le projet de loi visait « la protection des intérêts économiques et scientifiques fondamentaux de la France ».

Certains parlementaires, dénonçant le caractère trop général de ces notions d'intérêts fondamentaux, ont privilégié une rédaction s'inspirant de celle du Livre IV du Code pénal et notamment de son article 410-1 qui vise explicitement la « sauvegarde des éléments essentiels du potentiel scientifique et économique [de la Nation] » (Assemblée nationale, 2e séance, 13 juin 1991 ; Sénat du 25 juin 1991).

D'autres parlementaires ont fait valoir que « la possibilité d'interceptions de sécurité pour la protection des intérêts économiques et scientifiques fondamentaux d'un État est reconnue par la CEDH, dont le texte est d'ailleurs moins restrictif que le projet de loi, puisqu'il se réfère à la notion de "bien-être économique" » ; « [...] il est nécessaire que l'État dispose de moyens d'information et d'action adaptés aux menaces résultant de l'internationalisation des activités économiques » (François Massot, rapport de la Commission des lois de l'Assemblée nationale, 6 juin 1991).

« L'article 410-1 susvisé permet d'étendre la protection du Code pénal non seulement aux différents secteurs de l'économie au sens étroit du terme mais également à la recherche scientifique et aux innovations techniques ou technologiques sur lesquelles reposent précisément la force ou la compétitivité du pays. »

L'article 410-1 du Code pénal est suivi des articles 411-1 à 411-11 qui incriminent les différentes atteintes à ces intérêts au titre desquelles on relève plus particulièrement les infractions des articles 411-5 à 411-8 relatives aux différentes formes d'intelligence avec une puissance étrangère (article 411-5) et à la livraison d'informations à celle-ci (article 411-6 à 411-8).

Toute forme d'espionnage, y compris économique comme le transfert illicite de technologie, est clairement incriminée par ces articles, où est effectivement visée, la fourniture de procédés.

Cette fourniture peut être le fait d'auteurs divers (ingénieurs, agents de renseignement de pays tiers, « honorables correspondants », officines « spécialisées » dans l'espionnage économique) et être destinée non seulement à des services de renseignements de pays tiers (« puissances étrangères ») mais également à des entreprises ou des organisations étrangères.

Ce transfert illicite d'un procédé de fabrication, détenu exclusivement par un groupe national leader dans sa spécialité, est bien de nature à porter gravement atteinte aux éléments essentiels du potentiel scientifique et économique de la France. Il constitue sans aucun doute une atteinte aux intérêts fondamentaux de la Nation. Les éléments constitutifs d'une suspicion de commission du délit visé à l'article 411-7 du Code pénal, dont on remarquera qu'il constitue un mode original de répression de la tentative (le recueil des informations sans livraison de celles-ci est en soi punissable), sont réunis. En ce cas, l'interception de sécurité est parfaitement fondée en droit.

Il résulte de ces incriminations pénales qu'en dépit de la définition extensive donnée au concept d'intelligence économique, les interceptions sollicitées sous le motif « sauvegarde des éléments essentiels du potentiel scientifique et économique de la France », dont la formulation est directement reprise du Code pénal, correspondent à des faits précis et à des infractions prévues par le législateur.

La jurisprudence de la Commission, pour ce qui concerne ce motif, s'efforce à une synthèse :
– du dispositif normatif pénal ;
– du principe fondamental posé par la loi du 10 juillet 1991 de ce que les interceptions de sécurité relèvent exclusivement de la police administrative, et en conséquence des actions de prévention, et non des démarches actives préconisées par une partie de la doctrine née de l'intelligence économique ;
– de la conciliation entre la protection de notre patrimoine scientifique et économique et la nécessaire préservation de la « vie des affaires », protégée juridiquement dans une zone européenne où le libre-échange représente une valeur constitutive.

Ainsi la CNCIS retient les critères suivants : les interceptions de sécurité sollicitées sous le motif « sauvegarde des éléments essentiels du potentiel scientifique et économique de la France » doivent, d'une part, répondre à une menace (infraction issue du dispositif 411-1 à 411-11 du Code pénal) vérifiable traduisant une intention de nuire aux intérêts d'une entreprise française, d'autre part, la personne dont il est demandé d'intercepter les communications doit être clairement impliquée dans cette menace. L'activité de l'entreprise menacée doit enfin être liée à

la défense de notre indépendance nationale au sens de l'article 5 de la Constitution de la Ve République ou à la sécurité nationale.

Le décret 2005-1739 du 30 décembre 2005 réglementant les relations financières avec l'étranger [...] est venu ainsi définir en ses articles 2 et 3 des secteurs d'activité dont l'intérêt justifie la surveillance de leur financement au moyen d'investissements étrangers. Une telle définition peut, par analogie, représenter un travail d'approche qualitative des secteurs constituant les « éléments essentiels du potentiel scientifique et économique de la France ».

Prévention du terrorisme

Les textes en matière de police administrative renvoient pour ce motif au Livre IV du Code pénal et à l'article 421-1 qui incrimine spécialement certaines infractions quand celles-ci sont commises « intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur ».

Quand l'infraction commise répond aux conditions posées par cet article, il en découle d'importantes conséquences au plan de la procédure et de la répression. Ainsi sont modifiés les régimes de la garde à vue et des perquisitions, les règles de compétence des juridictions et de composition du tribunal, les régimes de prescription de l'action publique et de la peine, le quantum des peines principales et complémentaires encourues. Compte tenu de l'ensemble des dispositions dérogatoires figurant notamment aux articles 421-1 et suivants du Code pénal, la qualification d'une infraction d'acte de terrorisme, au sens de l'article 421-1 du Code pénal, revêt une particulière gravité et doit correspondre à toutes les conditions posées dans la définition légale de l'incrimination.

Les infractions ne peuvent être qualifiées d'actes de terrorisme que si elles ont bien été commises intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur. S'il est admis que l'acte peut être commis par un homme seul, il doit avoir été entrepris dans le but d'intimider ou de terroriser tout ou partie de la population.

Les termes de cette définition ont été précisés dans une circulaire du garde des Sceaux du 10 octobre 1986 (crim. 86-21-F. 1) et reprise par la doctrine (*cf. Jurisclasseur pénal* rubrique «Terrorisme »).

Cette « entreprise », selon cette circulaire, qui reprend les interventions du garde des Sceaux à l'Assemblée nationale (*JO* du 8 août 1986, p. 4125) et au Sénat (*JO* du 8 août 1986, p. 3795 et 3796), suppose « l'existence d'un dessein formé ou d'un plan concerté se traduisant par des efforts coordonnés en vue de l'objectif à atteindre. La notion d'entreprise

exclut l'improvisation ; elle suppose des préparatifs et un minimum d'organisation (établissement d'un plan d'action, rassemblement de moyens matériels, mise en place d'un dispositif de repli, rédaction de communiqué de revendication) ».

Un certain nombre d'actes relevant de l'expression politique violente pourraient répondre à cette définition comme l'organisation d'incidents en fin de manifestations, le démontage ou le sac symbolique de locaux publics ou privés. Toutefois, pour recevoir la qualification de terroristes, ces actes doivent avoir été commis avec la volonté de troubler gravement l'ordre public par l'intimidation ou la terreur, la gravité du trouble consistant dans la peur collective que l'on cherche à répandre dans la population ou partie de celle-ci afin de promouvoir une cause ou faciliter le succès d'une revendication.

Force est de constater que n'importe quelle action d'expression ou de revendication politique extrême, même violente et susceptible de troubler l'ordre public, ne saurait être qualifiée de terroriste. À la limite, la menace qu'elle peut faire peser sur les personnes et les biens, s'agissant d'une entreprise organisée et planifiée utilisant des moyens virulents peut relever dans certaines circonstances précises de la « criminalité organisée ». Ainsi les « casseurs » qui profitent d'une manifestation politique relèvent-ils de la criminalité organisée dès lors qu'ils constituent un groupe structuré. En revanche, même ce dernier motif ne peut être invoqué pour justifier des interceptions de sécurité à l'encontre de personnes impliquées dans des mouvements politiques extrêmes, pour la seule raison qu'ils contestent radicalement les fondements de notre organisation politique ou économique. Les agissements de ces mouvements relèvent, en effet, soit de poursuites pénales (provocations fondées sur des motivations raciales ou religieuses), soit du maintien de l'ordre public.

L'article L. 241-2 du Code de la sécurité intérieure (ancien article 3 de la loi du 10 juillet 1991) dispose que les interceptions de sécurité peuvent être autorisées pour la « prévention du terrorisme ». Les interceptions vont donc se situer en amont du passage à l'acte afin d'en empêcher la commission.

Il est possible d'autoriser la surveillance ciblée des individus les plus radicalisés afin de détecter à temps par exemple une dérive de type « brigadiste » sans entrer pour autant dans une police de l'opinion. Il faut caractériser une association de malfaiteurs en relation avec une entreprise terroriste en accumulant les indices sur la logistique mise en place (réseaux de financement fondés sur le don plus ou moins librement consenti, exploitation de commerces ne respectant pas la législation du travail, voire le crime organisé ; réseaux d'hébergement clandestin, d'infiltration ou d'exfiltration, caches d'armes, communauté de vie à caractère conspiratif) avant que celle-ci ne soit activée pour planifier un ou plusieurs attentats ou que ces faits ne relèvent de l'autorité judiciaire, seule compétente pour poursuivre ces faits.

Il faut pouvoir autoriser la surveillance de terreaux ciblés, sur lesquels la pensée terroriste peut éclore (dérive communautariste à caractère sectaire et vindicatif, endoctrinement de mineurs) sans porter atteinte à la liberté d'opinion telle que protégée par les articles 10 et 11 de la Déclaration des droits de l'homme de 1789.

La frontière est délicate à tracer *a priori*. Néanmoins, les cadres juridiques européens et nationaux contribuent à guider la réflexion de la Commission en ce domaine. Ainsi, certains mouvements sont cités par les décisions du Conseil de l'Union européenne en la matière.

Par ailleurs, la préparation en France d'actes à caractère terroriste devant être commis à l'étranger est susceptible, comme telle, de recevoir une qualification pénale (*cf.* article 113-2 al. 2 du Code pénal : « […] l'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire ») et entre naturellement dans le champ de ce motif légal d'interception.

Enfin, la loi nº 2012-1432 relative à la sécurité et à la lutte contre le terrorisme du 21 décembre 2012 renforce les sanctions contre ceux qui se rendent coupables d'apologie ou de provocation au terrorisme sur Internet.

Elle prévoit la poursuite par la justice française des actes de terrorisme commis à l'étranger par des Français ou des personnes résidant habituellement en France, en permettant d'incriminer les personnes ayant participé à des camps d'entraînement terroristes à l'étranger alors même qu'elles n'auront pas commis d'actes répréhensibles sur le territoire français.

Ces récentes modifications du cadre pénal national emportent des conséquences sur la définition et la déclinaison du motif « prévention du terrorisme » à partir duquel peut être autorisé et mis en œuvre, dans le cadre de la police administrative, une interception de sécurité ou un recueil de données techniques de communications.

Prévention de la criminalité et de la délinquance organisées

Comme les chiffres le montrent depuis de nombreuses années, en dépit de l'acuité de la menace terroriste, le premier motif de demandes initiales d'interceptions de sécurité reste la prévention de la criminalité et de la délinquance organisées.

L'essentiel des dossiers concerne les grands trafics tels que la livraison attendue par mer, terre ou air de stupéfiants, l'escroquerie à travers la contrebande d'objets contrefaits ou le repérage en vue d'attaques

d'établissements bancaires ou de transport de fonds, ou plus récemment encore l'économie souterraine.

Il apparaît aussi de plus en plus nettement que certains groupes activistes recourent volontiers à la criminalité de profit pour financer leurs filières et les attentats projetés. La Commission retient alors la finalité terroriste quand celle-ci est connue.

Ce concept, il y a peu, n'existait pas strictement à l'identique dans le Code pénal. Celui-ci traitait des infractions « commises en bande organisée ». La loi du 9 mars 2004 cependant a consacré dans le Livre quatrième du Code de procédure pénale un Titre 25e à la « procédure applicable à la criminalité et à la délinquance organisées », concernant l'ensemble des infractions aggravées par la circonstance de commission en bande organisée (*cf.* article 706-73 du Code de procédure pénale).

Il est donc permis de dire que le champ couvert aujourd'hui par l'article 706-73 du Code de procédure pénale recouvre désormais totalement celui couvert par l'article L. 241-2 du Code de la sécurité intérieure (ancien article 3 de la loi du 10 juillet 1991).

La CNCIS a très tôt apporté dans son rapport public une définition de ce motif au regard des interceptions de sécurité (*cf.* rapport 1994, p. 18 ; rapport 1995, p. 30). Elle a rappelé que cette définition résultait de celle retenue par la commission Schmelck chargée de proposer un cadre légal aux interceptions de sécurité, et par le Code pénal, notamment dans son article 132-71.

La commission Schmelck, dont les travaux sont à l'origine de la loi du 10 juillet 1991, envisageait de légaliser les interceptions de sécurité pour « la prévention du grand banditisme et du crime organisés ». Elle entendait par là se référer à des infractions qui avaient justifié, au plan administratif, la création d'offices spécialisés tels que l'Office central pour la répression du banditisme (OCRB)[1]. La Commission souhaitait faciliter la lutte en amont contre la grande criminalité.

L'article 132-71 du Code pénal, en définissant les circonstances aggravantes de certains crimes et délits, caractérise la bande organisée comme « tout groupement formé ou toute entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou plusieurs infractions ». Cette définition est également celle de l'association de malfaiteurs.

À l'entrée en vigueur du Nouveau Code pénal, les infractions pour lesquelles pouvait être retenue la circonstance aggravante de commission en bande organisée étaient relativement réduites et concernaient les formes graves du banditisme (trafic de stupéfiants, proxénétisme, enlèvement, racket, etc.).

1) Remplacé par l'Office central de lutte contre le crime organisé (OCLCO) depuis 2006.

Depuis le 1er mars 1994, la liste s'est allongée, spécialement avec l'entrée en vigueur de la loi no 2004-204 du 9 mars 2004 (dite Perben II) et des lois qui, depuis, sont venues la compléter.

« La plus redoutable menace – disait en 2004 le garde des Sceaux de l'époque – est celle du crime organisé dans ses formes diverses. À ceux qui choisissent délibérément de s'organiser dans le crime, la société doit répondre par une vigoureuse fermeté pénale. » Criminalité et délinquance organisées et infractions aggravées par la circonstance de commission en bande organisée sont donc bien des notions similaires.

La bande organisée est le groupement, la réunion de plusieurs malfaiteurs. L'élément constitutif qui, au plan pénal, va permettre de distinguer la commission en bande organisée de la simple réunion, c'est, précisément, l'organisation. Dans la simple réunion, il n'y a ni hiérarchie, ni distribution des rôles, ni entente préalable en vue de commettre des infractions. La réunion est fortuite, elle est une action collective inorganisée.

La commission en bande organisée suppose au contraire la préméditation. Elle suppose également un nombre de personnes supérieur à deux, chiffre qui suffit en revanche à caractériser la réunion.

Cette définition correspond à l'approche internationale du phénomène criminel organisé.

Ainsi, la convention des Nations unies contre la criminalité transnationale dite « convention de Palerme » du 15 novembre 2000, signée par la France le 12 décembre 2000 et ratifiée le 29 octobre 2002 stipule que :
– l'expression « groupe criminel organisé » désigne un groupe structuré de trois personnes ou plus existant depuis un certain temps et agissant de concert dans le but de commettre une ou plusieurs infractions graves pour en tirer directement ou indirectement un avantage financier ou un autre avantage matériel ;
– l'expression « infraction grave » désigne un acte constituant une infraction passible d'une peine privative de liberté dont le maximum ne doit pas être inférieur à quatre ans ou d'une peine plus lourde ;
– l'expression « groupe structuré » désigne un groupe qui ne s'est pas constitué au hasard pour commettre immédiatement une infraction et qui n'a pas nécessairement de rôles formellement définis pour ses membres, de continuité dans sa composition ou de structure élaborée.

Cette intégration de critères internationaux retenus dans la définition de la criminalité organisée (et notamment le nombre minimal de participants fixé à trois) a fait l'objet d'une « validation » par le Conseil constitutionnel lors de sa décision du 2 mars 2004 (considérants 13 et 14) relative à l'examen de la notion de criminalité organisée dans la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.

Pénalement, la circonstance de commission en bande organisée aggrave sensiblement plus les faits que la circonstance de simple réunion. Ainsi, le vol en réunion est puni de sept ans d'emprisonnement et le vol en bande organisée de quinze ans de réclusion criminelle (article 311-9 du Code pénal).

Ce qui caractérise par conséquent la « criminalité et la délinquance organisées », c'est à la fois la gravité des peines encourues et le degré d'organisation, notamment le nombre de personnes sciemment impliquées dans le processus criminel.

La majeure partie des projets d'interceptions soumis à la Commission répond effectivement à ces critères. Marginalement toutefois, la Commission note que quelques demandes ne revêtent pas cette gravité manifeste. Dans ces hypothèses, le caractère organisé au sens de l'article 132-71 du Code pénal n'est pas avéré et relève plus, tant par le faible degré d'entente que par le faible nombre de participants – au titre desquels on ne saurait ranger les « clients » dans, par exemple, l'hypothèse d'une revente de produits stupéfiants – d'une qualification de commission en réunion. En revanche, le nombre de clients estimés ou les quantités vendues sont un bon indice de la gravité des faits supposés.

L'organisation ne doit pas cependant être nécessairement totalement « professionnelle ». Le réseau constitué d'un fournisseur, de plusieurs « dealers », chacun responsable de son territoire, et de petits guetteurs bénévoles, entre bien dans la qualification de groupe criminel organisé au même titre que le cartel international de type mafieux.

La Commission a toujours réservé le recours à ce motif légal à des agissements d'une gravité certaine, souvent tendus par la recherche d'un avantage financier ou matériel et menés par de véritables structures organisées composées de plus de deux acteurs, participant d'une entente préalable caractérisant une préméditation criminelle et écartant de fait la commission fortuite d'une infraction à la faveur de la circonstance aggravante de réunion.

Ici encore, la position de la Commission représente une synthèse des dispositifs pénaux qui sont venus constituer le droit positif applicable à cette matière :
– notion de bande organisée au sens de l'article 132-71 du Code pénal ;
– notion d'association de malfaiteurs au sens de l'article 450-1 du Code pénal ;
– notion de « criminalité organisée » au sens de la loi du 9 mars 2004 précitée.

Sur le fondement de ces définitions de la bande organisée et de l'association de malfaiteurs, constatant le caractère exceptionnel de certains projets criminels ainsi que la gravité des atteintes aux intérêts fondamentaux de la Nation, la commission plénière a pu émettre des avis favorables pour des demandes portant sur des objectifs susceptibles

de commettre des infractions dont la nature et les conditions de leur commission, pouvaient porter atteinte à la vie et à la santé publique, alors que ces infractions ne sont explicitement visées à l'article 706-73 du Code de procédure pénale.

L'ampleur du trafic présumé, les modalités de commission des infractions projetées (notamment leur aspect international), les intérêts mis en cause par ces infractions, strictement identiques à ceux protégés par les incriminations de l'article 706-73, ont fondé ces avis de la Commission, en ce que les faits revêtaient le caractère exceptionnel visé par la loi pour autoriser une interception de sécurité.

S'agissant d'une menace particulièrement grave, et en l'absence d'autres moyens de recueil de renseignements, ces demandes apparaissent conformes aux principes de proportionnalité et de subsidiarité régissant les mesures d'investigation spéciales comme l'interception de sécurité, définies par la loi.

Prévention de la reconstitution ou du maintien de groupements dissous

Ce motif est directement lié à la mise en œuvre des dispositions de l'ancienne loi du 10 janvier 1936 sur les groupes de combat et les milices privées, désormais abrogée [1] et codifiée à l'article L. 212-1 du Code de la sécurité intérieure.

Ce texte dispose que sont dissous, par décret en conseil des ministres, toutes les associations ou groupements de fait :
1) Qui provoquent à des manifestations armées dans la rue.
2) Ou qui présentent, par leur forme et leur organisation militaires, le caractère de groupes de combat ou de milices privées.
3) Ou qui ont pour but de porter atteinte à l'intégrité du territoire national ou d'attenter par la force à la forme républicaine du Gouvernement.
4) Ou dont l'activité tend à faire échec aux mesures concernant le rétablissement de la légalité républicaine.
5) Ou qui ont pour but soit de rassembler des individus ayant fait l'objet de condamnation du chef de collaboration avec l'ennemi, soit d'exalter cette collaboration.
6) Ou qui, soit provoquent à la discrimination, à la haine ou à la violence envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée, soit propagent des idées

1) Par l'ordonnance no 2012-351 du 12 mars 2012.

ou théories tendant à justifier ou encourager cette discrimination, cette haine ou cette violence.
7) Ou qui se livrent, sur le territoire français ou à partir de ce territoire, à des agissements en vue de provoquer des actes de terrorisme en France ou à l'étranger.

Depuis 1936, près d'une centaine d'organisations ont ainsi fait l'objet d'une dissolution sur la base de ces dispositions légales.

Les interceptions de sécurité fondées sur ce motif suppose que l'objectif soit suspecté d'implication directe et personnelle dans des activités laissant présumer une volonté de reconstituer ou maintenir un groupement dissous, sans pour autant que le service demandeur dispose des éléments suffisants pour caractériser l'un des délits prévus et réprimés par la section 4 du chapitre Ier du Titre III du Livre IV du Code pénal[1].

1) Les articles 431-13 à 431-21 du Code pénal portent sur le maintien ou la reconstitution d'une association ou d'un groupement dissous en application de l'article L. 212-1 du Code de la sécurité intérieure, ou l'organisation de ce maintien ou de cette reconstitution, ainsi que l'organisation d'un groupe de combat.

Chapitre 2

Avis et préconisations de la Commission portant sur les demandes en matière d'interceptions de sécurité et de recueil des données techniques de communications

• Préalablement, il convient de rappeler le champ des demandes relevant du régime de protection des lois du 10 juillet 1991 et du 23 janvier 2006. À ce titre, elles relèvent des avis et du contrôle de la CNCIS.

Concernant ce champ d'application, la Commission en a régulièrement rappelé les limites par référence aux dispositions de l'article 20 de la loi du 10 juillet 1991 devenu l'article L. 241-3 du Code de la sécurité intérieure[1].

Par cet article, le législateur a entendu réserver une exception au principe du contrôle des interceptions de sécurité et du recueil des données techniques de communication par la CNCIS, en ce que les mesures mises en œuvre sur le fondement de cet article, s'inscrivent dans le cadre

1) Voir rapport d'activité 2011-2012 p. 40.

de la mission de surveillance générale du domaine radioélectrique, par opérations aléatoires de balayage des fréquences, pour la défense des intérêts nationaux. « Ces techniques réalisées dans le cadre de la mission générale de défense et ne visant pas de communications individualisables ne peuvent être considérées comme des ingérences de l'autorité publique dans l'exercice par toute personne de son droit au respect de sa correspondance au sens de l'article 8 de la CEDH » (Commission des lois du Sénat 19 juin 1991).

La Commission a rappelé la primauté du principe de libertés publiques sur l'évolution technique en indiquant que l'exception à son contrôle prévue par l'article 20 devait s'interpréter strictement : «Toute interception de correspondance échangée par la voie des télécommunications, qui n'entre pas dans le champ de l'article 20, est soumise quel que soit le mode de transmission filaire ou hertzien aux conditions et aux procédures fixées par la loi du 10 juillet 1991 ».

• Le contenu et la forme des demandes ainsi que la nature des contrôles varient selon qu'il s'agit d'interceptions du contenu des communications électroniques ou de recueillir les données techniques de ces correspondances, soit le contenant ou l'accessoire de la communication.

Les données techniques ne relèvent pas du même régime de protection en ce qu'elles ne permettent pas d'accéder et de connaître le contenu des correspondances et sont, à ce titre, moins attentatoires au secret des correspondances privées.

Pour ce qui concerne la Commission et le contrôle qu'elle exerce sur ce type de données, deux cadres légaux distincts sont mis en œuvre :
– l'article L. 244-2 du Code de la sécurité intérieure (ancien article 22 de la loi du 10 juillet 1991) pour l'ensemble des atteintes à la sécurité et aux intérêts fondamentaux prévus par la loi ;
– l'article 6 de la loi du 23 janvier 2006 permettant l'accès à ce type de mesure pour la seule prévention des actes de terrorisme et pour les services du ministère de l'Intérieur.

La CNCIS a, sur le fondement des dispositions de ces articles, défini une procédure de contrôle reposant sur les principes suivants :
– la centralisation, le traitement, et la validation, par le GIC pour les demandes fondées sur l'article L. 244-2 du Code de la sécurité intérieure, par la « personnalité qualifiée » pour les demandes relevant de l'article 6 de la loi du 23 janvier 2006 ;
– le contrôle *a posteriori* hebdomadaire de l'intégralité de ces demandes par la CNCIS ;
– la possibilité pour le GIC, comme pour la « personnalité qualifiée », de solliciter des renseignements complémentaires, et pour la Commission de recourir aux avis, aux recommandations, et aux droits de suite comme en matière d'interceptions de sécurité.

Les mesures sont classées selon la nature des informations qu'elles permettent de recueillir et l'importance de leur caractère intrusif dans la correspondance et la vie privées. Les exigences de rédaction, d'informations et de motivation des demandes sont déclinées en fonction de cette classification. Elles sont graduées en fonction de la catégorie des données concernées, selon qu'il s'agit de simples mesures d'identification ou de recueillir l'historique la localisation des cellules ou le détail du trafic.

La nature des contrôles exercés par la Commission pour chaque requête portant sur les données techniques de communications, est définie par rapport à cette classification et selon l'étendue de l'intrusion dans le contenant et les accessoires de la communication électronique.

Néanmoins, les principes généraux retenus pour les demandes d'interceptions de sécurité sont appliqués au recueil des données techniques de communication, tant en ce qui concerne la forme que le fond de la requête.

Les critères de la motivation de la demande

Chaque semaine, la Commission est amenée à donner son avis sur plus d'une centaine de demandes initiales ou de renouvellement d'interceptions de sécurité. En outre, et comme cela a déjà été indiqué dans les éléments chiffrés relatant son activité, elle statue quotidiennement sur des demandes présentées sous la forme de l'urgence absolue.

Dans le cadre de l'élaboration de ses avis, la Commission examine plus particulièrement au niveau des motivations les critères principaux suivants :
– la qualification juridique des faits au regard des motifs légaux ;
– les présomptions d'implication directe et personnelle de l'objectif dans les projets d'atteintes et d'infractions ou les menaces ;
– la proportionnalité qui permet de mesurer le rapport entre le but recherché et l'action sollicitée. La gravité du risque et l'importance des intérêts en jeu doivent être à la mesure de l'atteinte à la vie privée que constitue la surveillance de la correspondance par voie de communications électroniques ou l'exploitation des données de correspondances électroniques, et la justifier pleinement ;
– la subsidiarité qui permet de s'assurer de l'absolue nécessité de recourir matériellement à l'interception ou au recueil de données techniques de communication, et de vérifier que le but recherché ne peut pas être aussi bien atteint par d'autres moyens.

Il résulte de l'application de ces critères que la motivation doit être suffisante, pertinente et sincère.

Une motivation suffisante

La motivation doit être suffisante en quantité, mais aussi en qualité :

• En quantité

Quelques lignes ne sauraient suffire. Les développements doivent permettre de cerner la personnalité de la cible, de développer un minimum les soupçons qui pèsent sur elle, et d'expliquer la nature et la gravité du danger qu'elle fait courir à la sécurité de l'État et aux citoyens. Ces informations permettent également à la Commission d'opérer un contrôle sur l'articulation juridique entre des éléments factuels relevant du comportement de la cible et le motif légal d'interception invoqué par le service.

Dans la majorité des cas, les « renseignements complémentaires » fournis à la demande de la Commission emporteront la conviction de cette dernière qui déplore dès lors une information initiale insuffisante.

• En qualité

La motivation doit absolument :
– faire ressortir les présomptions d'implication directe et personnelle de la cible. Quel que soit le motif, l'implication directe et personnelle de l'objectif dans des agissements attentatoires à notre sécurité, doit être présumée ;
– ne pas se référer à un comportement purement hypothétique de celle-ci ou à des comportements généraux de groupements auxquels appartiendrait l'objectif.

Ainsi une demande trop éloignée d'une implication directe et personnelle de la cible dans des faits participant du motif invoqué peut recevoir un avis négatif comme par exemple une demande où la démonstration de cette implication ne repose que sur un « relationnel » avec d'autres individus.

Une motivation pertinente

L'examen de cette pertinence porte sur trois points :
– la motivation doit être exclusivement tournée vers la vocation préventive voulue par le législateur de 1991 pour les interceptions de sécurité. Outil de renseignement, ces mêmes interceptions ne peuvent être utilisées pour l'élucidation de faits passés relevant de l'autorité judiciaire ;
– corrélativement, la motivation doit exclusivement se référer à des investigations participant de l'activité de renseignement et en aucun cas pouvoir générer un « risque d'interférence » avec une action judiciaire déjà déclenchée ;
– enfin, les soupçons qui pèsent sur la cible doivent nécessairement être en relation directe avec le motif. Ainsi un comportement dont la description reste floue, vague, imprécise et non « rattachable » au travail d'articulation juridique déjà décrit prive la demande de toute pertinence.

La Commission a poursuivi son inscription dans une volonté de dialogue avec les services demandeurs. Cette démarche s'est traduite par une nette augmentation des réunions bilatérales avec ces mêmes services. Elle s'est également matérialisée, au stade de l'examen de leurs demandes, par une logique d'avis moins binaire (avis favorable/défavorable). De fait, le nombre d'observations a encore crû, comme les demandes de renseignements complémentaires et les limitations de la durée d'interception sollicitée. Les avis défavorables sont stabilisés à une cinquantaine par an. À ce chiffre des avis défavorables « bruts », il convient d'ajouter deux techniques d'observation déjà répertoriées dans le rapport d'activité 2008 qui peuvent s'apparenter à « l'avis négatif » :

• la recommandation adressée au Premier ministre visant à l'interruption de l'interception en cours d'exploitation qui résulte de l'examen exhaustif des « productions » (transcriptions) opérées à partir d'une interception. En moyenne, depuis 1991, il y est fait recours une dizaine de fois par an. Elles sont suivies par le Premier ministre ;

• la « préconisation d'interruption » adressée par la Commission au service utilisateur en cours d'exploitation. Elle résulte du même examen des productions et procède d'un dialogue constructif mené directement avec les services utilisateurs pour un réexamen de l'interception et de son exploitation par rapport à l'autorisation et aux dispositions légales. Cela concerne, en moyenne une cinquantaine de mesures par an, qui sont toutes suivies d'une interruption, à l'initiative du service, dans un bref délai.

Une motivation sincère

Il importe aussi de s'assurer que le motif légal invoqué ne dissimule pas d'autres préoccupations ou des objectifs non visés par la loi. L'interception doit être sollicitée exclusivement pour les faits articulés, et non pour une raison autre qui ne relèverait d'aucun motif légal, quelle que soit par ailleurs la véracité des faits rapportés. C'est la notion de demande sincère.

Le mensonge caractérisé et délibéré dans la présentation des motifs de la demande entraîne l'illégalité de l'interception qui serait autorisée par le Premier ministre à la suite de l'avis rendu par la Commission sur le fondement d'informations mensongères et dont les véritables objectifs seraient dissimulés.

Le caractère illégal de l'interception et les suites pénales qui sont susceptibles d'en découler en matière d'atteintes au secret des correspondances sont identiques lorsque certaines informations soutenant la demande sont partiellement exactes, sont amplifiées, ou lorsque des hypothèses ou des soupçons sont présentés comme des faits établis. La Commission rappelle que, s'agissant de police administrative préventive, la loi exige des présomptions d'implication. Quand les atteintes

sont certaines et établies, le recours au dispositif administratif est exclu. Les poursuites pénales sont exclusives, tel que le rappelle le Conseil constitutionnel lorsqu'il souligne « la primauté de l'autorité judiciaire ».

Troisième partie

ÉTUDES ET DOCUMENTS

Chapitre I

Présentation ordonnée des textes relatifs aux missions de la Commission

Première mission : les interceptions de communications

Avant de reproduire certaines dispositions spécifiques ou communes aux différents types d'interception, il convient de rappeler le principe du secret des correspondances émises par la voie des « communications électroniques » posé par l'article 1er de la loi nº 91-646 du 10 juillet 1991, devenu l'article L. 241-1 du Code de la sécurité intérieure : « Le secret des correspondances émises par la voie des communications électroniques est garanti par la loi. Il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci. »

Les interceptions légales de correspondances émises par la voie des « communications électroniques » sont de deux types : judiciaires et de sécurité.

S'agissant des interceptions judiciaires, le pluriel est employé à dessein depuis l'entrée en vigueur des lois nº 2002-1138 du 9 septembre 2002 et 2004-204 du 9 mars 2004, modifiée dernièrement par la loi nº 2011-267 du 11 mars 2011.

En effet, aux interceptions en matière criminelle et correctionnelle prévues par les articles 100 à 100-7 du Code de procédure pénale, s'ajoutent celles prévues par les dispositions suivantes du même code :
– article 74-2 (recherche d'une personne en fuite) ;
– article 80-4 (recherche des causes de la mort ou d'une disparition présentant un caractère inquiétant) ;
– article 706-95 (criminalité et délinquance organisées) ;
– article 727-1 (écoute, enregistrement et interruption des conversations téléphoniques des détenus).

Pour des raisons de clarté de présentation les dispositions relatives à ces interceptions seront présentées à la suite de celles des articles 100 à 107 du Code de procédure pénale auxquels elles renvoient même si elles ne faisaient pas explicitement partie du Titre Ier de la loi de 1991, et ne figurent pas dans le Code de la sécurité intérieure.

La loi nº 91-646 du 10 juillet 1991 (abrogée depuis le 1er mai 2012 conformément à l'article 19, *20°*, de l'ordonnance nº 2012-351 du 12 mars 2012)

Il s'agit d'une loi fondatrice en matière de protection de secret des correspondances. Elle a créé la Commission nationale de contrôle des interceptions de sécurité.

Titre I (de la loi nº 91-646 du 10 juillet 1991 consolidée) : DES INTERCEPTIONS ORDONNÉES PAR L'AUTORITÉ JUDICIAIRE

Les interceptions ordonnées en matière criminelle et correctionnelle

Code de procédure pénale

Livre Ier : De l'exercice de l'action publique et de l'instruction

Titre III : Des juridictions d'instruction

Chapitre Ier : Du juge d'instruction : juridiction d'instruction du premier degré

Section III : Des transports, des perquisitions, des saisies et des interceptions de correspondances émises par la voie des télécommunications

Sous-section II : Des interceptions de correspondances émises par la voie des télécommunications

Article 100 – « En matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à deux ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications. Ces opérations sont effectuées sous son autorité et son contrôle.

La décision d'interception est écrite. Elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours. »

Article 100-1 – « La décision prise en application de l'article 100 doit comporter tous les éléments d'identification de la liaison à intercepter, l'infraction qui motive le recours à l'interception ainsi que la durée de celle-ci. »

Article 100-2 – « Cette décision est prise pour une durée maximum de quatre mois. Elle ne peut être renouvelée que dans les mêmes conditions de forme et de durée. »

Article 100-3 – « Le juge d'instruction ou l'officier de police judiciaire commis par lui peut requérir tout agent qualifié d'un service ou organisme placé sous l'autorité ou la tutelle du ministre chargé des télécommunications ou tout agent qualifié d'un exploitant de réseau ou fournisseur de services de télécommunications autorisé, en vue de procéder à l'installation d'un dispositif d'interception. »

Article 100-4 – « Le juge d'instruction ou l'officier de police judiciaire commis par lui dresse procès-verbal de chacune des opérations d'interception et d'enregistrement. Ce procès-verbal mentionne la date et l'heure auxquelles l'opération a commencé et celles auxquelles elle s'est terminée.

Les enregistrements sont placés sous scellés fermés. »

Article 100-5 – « Le juge d'instruction ou l'officier de police judiciaire commis par lui transcrit la correspondance utile à la manifestation de la vérité. Il en est dressé procès-verbal. Cette transcription est versée au dossier.

Les correspondances en langue étrangère sont transcrites en français avec l'assistance d'un interprète requis à cette fin.

À peine de nullité, ne peuvent être transcrites les correspondances avec un avocat relevant de l'exercice des droits de la défense.

À peine de nullité, ne peuvent être transcrites les correspondances avec un journaliste permettant d'identifier une source en violation de l'article 2 de la loi du 29 juillet 1881 sur la liberté de la presse.

Article 100-6 – « Les enregistrements sont détruits, à la diligence du procureur de la République ou du procureur général, à l'expiration du délai de prescription de l'action publique.

Il est dressé procès-verbal de l'opération de destruction. »

Article 100-7 – (*loi n° 95-125 du 8 février 1995)* – « Aucune interception ne peut avoir lieu sur la ligne d'un député ou d'un sénateur sans que le président de l'assemblée à laquelle il appartient en soit informé par le juge d'instruction.

Aucune interception ne peut avoir lieu sur une ligne dépendant du cabinet d'un avocat ou de son domicile sans que le bâtonnier en soit informé par le juge d'instruction. »

- Loi nº 93-1013 du 24 août 1993. « Les formalités prévues par le présent article sont prescrites à peine de nullité. »

Les interceptions ordonnées pour recherche d'une personne en fuite

Code de procédure pénale

Livre Ier : De l'exercice de l'action publique et de l'instruction

Titre II : Des enquêtes de contrôle d'identité

Chapitre Ier : Des crimes et des délits flagrants

Article 74-2 – « Les officiers de police judiciaire, assistés le cas échéant des agents de police judiciaire, peuvent, sur instructions du procureur de la République, procéder aux actes prévus par les articles 56 à 62 aux fins de rechercher et de découvrir une personne en fuite dans les cas suivants :
1) Personne faisant l'objet d'un mandat d'arrêt délivré par le juge d'instruction, le juge des libertés et de la détention, la chambre de l'instruction ou son président ou le président de la cour d'assises, alors qu'elle est renvoyée devant une juridiction de jugement ;
2) Personne faisant l'objet d'un mandat d'arrêt délivré par une juridiction de jugement ou par le juge de l'application des peines ;
3) Personne condamnée à une peine privative de liberté sans sursis supérieure ou égale à un an, lorsque cette condamnation est exécutoire ou passée en force de chose jugée. »

Si les nécessités de l'enquête pour rechercher la personne en fuite l'exigent, le juge des libertés et de la détention du tribunal de grande instance peut, à la requête du procureur de la République, autoriser l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications selon les modalités prévues par les articles 100, 100-1 et 100-3 à 100-7, pour une durée maximale de deux mois renouvelable dans les mêmes conditions de forme et de durée, dans la limite de six mois en matière correctionnelle. Ces opérations sont faites sous l'autorité et le contrôle du juge des libertés et de la détention […]. »

NB : les articles 695-36 et 696-21 du Code de procédure pénale étendent respectivement les dispositions de l'article 74-2 du même code au mandat d'arrêt européen et à la procédure d'extraction (*cf.* article 39 V et VI de la loi 2005-1549 du 12 décembre 2005 relative au traitement de la récidive des infractions pénales).

Les interceptions ordonnées pendant le déroulement de l'information pour recherche des causes de la mort ou d'une disparition de mineur, de majeur protégé ou présentant un caractère inquiétant

Code de procédure pénale (loi no 2002-1138 du 9 septembre 2002, article 66)

Livre Ier : De l'exercice de l'action publique et de l'instruction

Titre III : Des juridictions d'instruction

Chapitre Ier : Du juge d'instruction : juridiction d'instruction du premier degré

Section I : Dispositions générales

Article 80-4 – « Pendant le déroulement de l'information pour recherche des causes de la mort ou des causes d'une disparition mentionnée aux articles 74 et 74-1, le juge d'instruction procède conformément aux dispositions du chapitre Ier du Titre III du Livre Ier. Les interceptions de correspondances émises par la voie des télécommunications sont effectuées sous son autorité et son contrôle dans les conditions prévues au deuxième alinéa de l'article 100 et aux articles 100-1 à 100-7. Les interceptions ne peuvent excéder une durée de deux mois renouvelable.

Les membres de la famille ou les proches de la personne décédée ou disparue peuvent se constituer partie civile à titre incident. Toutefois, en cas de découverte de la personne disparue, l'adresse de cette dernière et les pièces permettant d'avoir directement ou indirectement connaissance de cette adresse ne peuvent être communiquées à la partie civile qu'avec l'accord de l'intéressé s'il s'agit d'un majeur et qu'avec l'accord du juge d'instruction s'il s'agit d'un mineur ou d'un majeur protégé. »

Les interceptions ordonnées en matière de criminalité et délinquance organisées

Code de procédure pénale

Livre IV : De quelques procédures particulières

Titre XXV : De la procédure applicable à la criminalité et à la délinquance organisées

Chapitre II : Procédure

Section V : Des interceptions de correspondances émises par la voie des télécommunications

Article 706-95 – « Si les nécessités de l'enquête de flagrance ou de l'enquête préliminaire relative à l'une des infractions entrant dans le champ d'application de l'article 706-73 l'exigent, le juge des libertés et de la détention du tribunal de grande instance peut, à la requête du procureur de la République, autoriser l'interception, l'enregistrement et la

transcription de correspondances émises par la voie des télécommunications selon les modalités prévues par les articles 100 deuxième alinéa, 100-1 et 100-3 à 100-7, pour une durée maximum d'un mois[1], renouvelable une fois dans les mêmes conditions de forme et de durée.

Ces opérations sont faites sous le contrôle du juge des libertés et de la détention […]. »

Les interceptions prévues par l'article 727-1 du Code de procédure pénale

Code de procédure pénale

Livre V : Des procédures d'exécution

Titre II : De la détention

Chapitre III : Des dispositions communes aux différents établissements pénitentiaires

Article 727-1 – Créé par la loi nº 2007-297 du 5 mars 2007 – article 72 *JORF* 7 mars 2007

« Aux fins de prévenir les évasions et d'assurer la sécurité et le bon ordre des établissements pénitentiaires ou des établissements de santé habilités à recevoir des détenus, les communications téléphoniques « des personnes détenues »[2] peuvent, à l'exception de celles avec leur avocat, être écoutées, enregistrées et interrompues par l'administration pénitentiaire sous le contrôle du procureur de la République territorialement compétent, dans des conditions et selon des modalités qui sont précisées par décret[3].

Les détenus ainsi que leurs correspondants sont informés du fait que les conversations téléphoniques peuvent être écoutées, enregistrées et interrompues.

Les enregistrements qui ne sont suivis d'aucune transmission à l'autorité judiciaire en application de l'article 40 ne peuvent être conservés au-delà d'un délai de trois mois. »

Titre II (de la loi nº 91-646 du 10 juillet 1991 consolidée) :
DES INTERCEPTIONS DE SÉCURITÉ

Article 3 – « Peuvent être autorisées, à titre exceptionnel, dans les conditions prévues par l'article 4, les interceptions de correspondances

1) La loi nº 2011-267 du 11 mars 2011 a fait passer la durée légale de quinze jours à un mois, renouvelable une fois.
2) Loi 2009-1436 du 24 novembre 2009, art. 97-II.
3) Décret nº 2010-1635 du 23 décembre 2010 portant application de la loi pénitentiaire et modifiant le Code de procédure pénale (troisième partie : Décrets).

émises par la voie des "communications électroniques" (loi nº 2004-669 du 9 juillet 2004) ayant pour objet de rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées. »

Article 4 – *modifié par l'article 6 II de la loi nº 2006-64 du 23 janvier 2006* –

« L'autorisation est accordée par décision écrite et motivée du Premier ministre ou de l'une des deux personnes spécialement déléguées par lui. Elle est donnée sur proposition écrite et motivée du ministre de la Défense, du ministre de l'Intérieur ou du ministre chargé des Douanes, ou de l'une des deux personnes que chacun d'eux aura spécialement déléguée.

Le Premier ministre organise la centralisation de l'exécution des interceptions autorisées. »

Article 5 – « Le nombre maximum des interceptions susceptibles d'être pratiquées simultanément en application de l'article 4 est arrêté par le Premier ministre.

La décision fixant ce contingent et sa répartition entre les ministères mentionnés à l'article 4 est portée sans délai à la connaissance de la Commission nationale de contrôle des interceptions de sécurité. »

Article 6 – « L'autorisation mentionnée à l'article 3 est donnée pour une durée maximum de quatre mois. Elle cesse de plein droit de produire effet à l'expiration de ce délai. Elle ne peut être renouvelée que dans les mêmes conditions de forme et de durée. »

Article 7 – « Dans les correspondances interceptées, seuls les renseignements en relation avec l'un des objectifs énumérés à l'article 3 peuvent faire l'objet d'une transcription.

Cette transcription est effectuée par les personnels habilités. »

Article 8 – « Il est établi, sous l'autorité du Premier ministre, un relevé de chacune des opérations d'interception et d'enregistrement. Ce relevé mentionne la date et l'heure auxquelles elle a commencé et celles auxquelles elle s'est terminée. »

Article 9 – « L'enregistrement est détruit sous l'autorité du Premier ministre, à l'expiration d'un délai de dix jours au plus tard à compter de la date à laquelle il a été effectué. Il est dressé procès-verbal de cette opération. »

Article 10 – « Sans préjudice de l'application du deuxième alinéa de l'article 40 du Code de procédure pénale, les renseignements recueillis ne peuvent servir à d'autres fins que celles mentionnées à l'article 3. »

Article 11 – « Les opérations matérielles nécessaires à la mise en place des interceptions dans les locaux et installations des services ou organismes placés sous l'autorité ou la tutelle du ministre chargé des "communications électroniques" ou des exploitants de réseaux ou fournisseurs de services de "communications électroniques" ne peuvent être effectuées que sur ordre du ministre chargé des "communications électroniques" ou sur ordre de la personne spécialement déléguée par lui, par des agents qualifiés de ces services, organismes, exploitants ou fournisseurs dans leurs installations respectives. »

Article 11-1 – *(introduit par l'article 31 de la loi nº 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne)* – « Les personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité sont tenues de remettre aux agents autorisés dans les conditions prévues à l'article 4, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies. Les agents autorisés peuvent demander aux fournisseurs de prestations susmentionnés de mettre eux-mêmes en œuvre ces conventions, sauf si ceux-ci démontrent qu'ils ne sont pas en mesure de satisfaire à ces réquisitions.

Le fait de ne pas déférer, dans ces conditions, aux demandes des autorités habilitées est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.

Un décret en Conseil d'État précise les procédures suivant lesquelles cette obligation est mise en œuvre ainsi que les conditions dans lesquelles la prise en charge financière de cette mise en œuvre est assurée par l'État. »

Article 12 – « Les transcriptions d'interceptions doivent être détruites dès que leur conservation n'est pas indispensable à la réalisation des fins mentionnées à l'article 3.

Il est dressé procès-verbal de l'opération de destruction.

Les opérations mentionnées aux alinéas précédents sont effectuées sous l'autorité du Premier ministre. »

Article 13 – « Il est institué une Commission nationale de contrôle des interceptions de sécurité. Cette commission est une autorité administrative indépendante. Elle est chargée de veiller au respect des dispositions du présent titre. Elle est présidée par une personnalité désignée, pour une durée de six ans, par le président de la République, sur une liste, de quatre noms, établie conjointement par le vice-président du Conseil d'État et le premier président de la Cour de cassation.

Elle comprend, en outre :
– un député désigné pour la durée de la législature par le président de l'Assemblée nationale ;
– un sénateur désigné après chaque renouvellement partiel du Sénat par le président du Sénat.

La qualité de membre de la Commission est incompatible avec celle de membre du Gouvernement. Sauf démission, il ne peut être mis fin aux fonctions de membre de la Commission qu'en cas d'empêchement constaté par celle-ci. Le mandat des membres de la Commission n'est pas renouvelable. En cas de partage des voix, la voix du président est prépondérante. Les agents de la Commission sont nommés par le président.

Les membres de la Commission désignés en remplacement de ceux dont les fonctions ont pris fin avant leur terme normal achèvent le mandat de ceux qu'ils remplacent. À l'expiration de ce mandat, par dérogation au septième alinéa ci-dessus, ils peuvent être nommés comme membre de la Commission s'ils ont occupé ces fonctions de remplacement pendant moins de deux ans.

Les membres de la Commission sont astreints au respect des secrets protégés par les articles 226-13, 226-14 et 413-10 du Code pénal pour les faits, actes ou renseignements dont ils ont pu avoir connaissance en raison de leurs fonctions. La Commission établit son règlement intérieur. »

Article 14 – « La décision motivée du Premier ministre mentionnée à l'article 4 est communiquée dans un délai de 48 heures au plus tard au président de la Commission nationale de contrôle des interceptions de sécurité.

Si celui-ci estime que la légalité de cette décision au regard des dispositions du présent titre n'est pas certaine, il réunit la Commission, qui statue dans les sept jours suivant la réception par son président de la communication mentionnée au premier alinéa.

Au cas où la Commission estime qu'une interception de sécurité a été autorisée en méconnaissance des dispositions du présent titre, elle adresse au Premier ministre une recommandation tendant à ce que cette interception soit interrompue.

Elle porte également cette recommandation à la connaissance du ministre ayant proposé l'interception et du ministre chargé des "communications électroniques".

La Commission peut adresser au Premier ministre une recommandation relative au contingent et à sa répartition visée à l'article 5.

Le Premier ministre informe sans délai la Commission des suites données à ses recommandations. »

Article 15 – « De sa propre initiative ou sur réclamation de toute personne y ayant un intérêt direct et personnel, la Commission peut procéder au contrôle de toute interception de sécurité en vue de vérifier si elle est effectuée dans le respect des dispositions du présent titre.

Si la Commission estime qu'une interception de sécurité est effectuée en violation des dispositions du présent titre, elle adresse au Premier ministre une recommandation tendant à ce que cette interception soit interrompue.

Il est alors procédé ainsi qu'il est indiqué aux quatrième et sixième alinéas de l'article 14. »

Article 16 – « Les ministres, les autorités publiques, les agents publics doivent prendre toutes mesures utiles pour faciliter l'action de la Commission. »

Article 17 – « Lorsque la Commission a exercé son contrôle à la suite d'une réclamation, il est notifié à l'auteur de la réclamation qu'il a été procédé aux vérifications nécessaires.

Conformément au deuxième alinéa de l'article 40 du Code de procédure pénale, la Commission donne avis sans délai au procureur de la République de toute infraction aux dispositions de la présente loi dont elle a pu avoir connaissance à l'occasion du contrôle effectué en application de l'article 15. »

Article 18 – « Les crédits nécessaires à la Commission nationale de contrôle des interceptions de sécurité pour l'accomplissement de sa mission sont inscrits au budget des services du Premier ministre. »

Article 19 – *modifié par l'article 6 de la loi nº 2006-64 du 23 janvier 2006* – « La Commission remet chaque année au Premier ministre un rapport sur les conditions d'exercice et les résultats de son activité, qui précise notamment le nombre de recommandations qu'elle a adressées au Premier ministre en application de l'article 4 de la présente loi et au ministre de l'Intérieur en application de l'article L. 34-1-1 du Code des postes et des communications électroniques et de l'article 6 de la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, ainsi que les suites qui leur ont été données. Ce rapport est rendu public.

Elle adresse, à tout moment, au Premier ministre les observations qu'elle juge utile. »

Titre III (de la loi nº 91-646 du 10 juillet 1991 consolidée) : DISPOSITIONS COMMUNES AUX INTERCEPTIONS JUDICIAIRES ET DE SÉCURITÉ

Article 20 – « Les mesures prises par les pouvoirs publics pour assurer, aux seules fins de défense des intérêts nationaux, la surveillance et le contrôle des transmissions empruntant la voie hertzienne ne sont pas soumises aux dispositions des Titres I et II de la présente loi. »

Article 21 – « Dans le cadre des attributions qui lui sont conférées par le Livre II du Code des postes et des "communications électroniques", le ministre chargé des "communications électroniques" veille notamment à ce que l'exploitant public, les autres exploitants de réseaux publics de "communications électroniques" et les autres fournisseurs de services de "communications électroniques" autorisés prennent les mesures nécessaires pour assurer l'application des dispositions de la présente loi. »

Article 22 – *(modifié par l'article 18 de la loi nº 96-659 du 26 juillet 1996 sur la réglementation des télécommunications)* – « Les juridictions compétentes pour ordonner des interceptions en application du Code de procédure pénale ainsi que le Premier ministre ou, en ce qui concerne l'exécution des mesures prévues à l'article 20, le ministre de la Défense ou le ministre de l'Intérieur, peuvent recueillir, auprès des personnes physiques ou morales exploitant des réseaux de "communications électroniques" ou fournisseurs de services de "communications électroniques", les informations ou documents qui leur sont nécessaires, chacun en ce qui le concerne, pour la réalisation et l'exploitation des interceptions autorisées par la loi.

La fourniture des informations ou documents visés à l'alinéa précédent ne constitue pas un détournement de leur finalité au sens de l'article 226-21 du Code pénal.

Le fait, en violation du premier alinéa, de refuser de communiquer les informations ou documents, ou de communiquer des renseignements erronés est puni de six mois d'emprisonnement et de 7 500 euros d'amende. Les personnes morales peuvent être déclarées responsables pénalement dans les conditions prévues par l'article 121-2 du Code pénal de l'infraction définie au présent alinéa. Les peines encourues par les personnes morales sont l'amende, suivant les modalités prévues par l'article 131-38 du Code pénal. »

Article 23 – « Les exigences essentielles définies au 12° de l'article L. 32 du Code des postes et des "communications électroniques" et le secret des correspondances mentionné à l'article L. 32-3 du même code ne sont opposables ni aux juridictions compétentes pour ordonner des interceptions en application de l'article 100 du Code de procédure pénale,

ni au ministre chargé des "communications électroniques" dans l'exercice des prérogatives qui leur sont dévolues par la présente loi. »

Article 24 – *cf.* article 226-3 du Code pénal (ex-article 371 du même code).

Article 226-3 – « Est puni des mêmes peines [un an d'emprisonnement et 45 000 euros d'amende] la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente, en l'absence d'autorisation ministérielle dont les conditions d'octroi sont fixées par décret en Conseil d'État, d'appareils conçus pour réaliser les opérations pouvant constituer l'infraction prévue par le deuxième alinéa de l'article 226-15 ou qui, conçus pour la détection à distance des conversations, permettent de réaliser l'infraction prévue par l'article 226-1 et figurant sur une liste dressée dans des conditions fixées par ce même décret. Est également puni des mêmes peines le fait de réaliser une publicité en faveur d'un appareil susceptible de permettre la réalisation des infractions prévues par l'article 226-1 et le second alinéa de l'article 226-15 du Code pénal lorsque cette publicité constitue une incitation à commettre cette infraction. »

Article 25 – *cf.* article 432-9 du Code pénal (ex-article 186-1 du même code).

Article 432-9 – « Le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, le détournement, la suppression ou l'ouverture de correspondances ou la révélation du contenu de ces correspondances, est puni de trois ans d'emprisonnement et de 45 000 euros d'amende.

Est puni des mêmes peines le fait, par une personne visée à l'alinéa précédent ou un agent d'un exploitant de réseau de "ouvert au public de communications électroniques" ou d'un fournisseur de services de "communications électroniques", agissant dans l'exercice de ses fonctions, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu. »

Article 26 – « Sera punie des peines mentionnées à l'article 226-13 1 du Code pénal toute personne qui, concourant dans les cas prévus par la loi à l'exécution d'une décision d'interception de sécurité, révélera l'existence de l'interception. »

Titre IV (de la loi nº 91-646 du 10 juillet 1991 consolidée) :
COMMUNICATION DES DONNÉES TECHNIQUES RELATIVES À DES COMMUNICATIONS ÉLECTRONIQUES

Article 27 – « La Commission nationale de contrôle des interceptions de sécurité exerce les attributions définies à l'article L. 34-1-1 du Code des postes et des communications électroniques et à l'article 6 de la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique en ce qui concerne les demandes de communication de données formulées auprès des opérateurs de communications électroniques et personnes mentionnées à l'article L. 34-1 du code précité ainsi que des prestataires mentionnés aux 1 et 2 du I de l'article 6 de la loi nº 2004-575 du 21 juin 2004 précitée. »

1) Substitué dans le Nouveau Code pénal à l'article 378, mentionné dans la loi du 10 juillet 1991.

Titre V (de la loi nº 91-646 du 10 juillet 1991 consolidée) :
DISPOSITIONS FINALES

Article 28 – « La présente loi entrera en vigueur le 1er octobre 1991. »

1.2. Le Titre IV « Interceptions de sécurité » du Livre II « Ordre et sécurité publics » du Code de la sécurité intérieure [1]

TITRE IV Interceptions de sécurité

---

* Il s'agit du texte applicable depuis le 1er mai 2012, date de l'abrogation de la loi du 10 juillet 1991, après la ratification, par le Parlement, de l'ordonnance nº 2012-351 du 12 mars 2012.

Chapitre Ier : Dispositions générales

Article L. 241-1

Le secret des correspondances émises par la voie des communications électroniques est garanti par la loi.

Il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci.

Article L. 241-2

Peuvent être autorisées, à titre exceptionnel, dans les conditions prévues par l'article L. 242-1, les interceptions de correspondances

émises par la voie des communications électroniques ayant pour objet de rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de l'article L. 212-1.

Article L. 241-3

Les mesures prises par les pouvoirs publics pour assurer, aux seules fins de défense des intérêts nationaux, la surveillance et le contrôle des transmissions empruntant la voie hertzienne ne sont pas soumises aux dispositions du présent titre, ni à celles de la sous-section 2 de la section 3 du chapitre Ier du Titre III du Livre Ier du Code de procédure pénale.

Article L. 241-4

Les exigences essentielles définies au 12° de l'article L. 32 du Code des postes et communications électroniques et le secret des correspondances mentionné à l'article L. 32-3 du même code ne sont opposables ni aux juridictions compétentes pour ordonner des interceptions en application de l'article 100 du Code de procédure pénale, ni au ministre chargé des « communications électroniques » dans l'exercice des prérogatives qui leur sont dévolues par le présent titre.

Chapitre II : Conditions des interceptions

Article L. 242-1

L'autorisation prévue à l'article L. 241-2 est accordée par décision écrite et motivée du Premier ministre ou de l'une des deux personnes spécialement déléguées par lui. Elle est donnée sur proposition écrite et motivée du ministre de la défense, du ministre de l'Intérieur ou du ministre chargé des Douanes, ou de l'une des deux personnes que chacun d'eux aura spécialement déléguées.

Le Premier ministre organise la centralisation de l'exécution des interceptions autorisées.

Article L. 242-2

Le nombre maximum des interceptions susceptibles d'être pratiquées simultanément en application de l'article L. 242-1 est arrêté par le Premier ministre.

La décision fixant ce contingent et sa répartition entre les ministères mentionnés à l'article L. 242-1 est portée sans délai à la connaissance de la Commission nationale de contrôle des interceptions de sécurité.

Article L. 242-3

L'autorisation mentionnée à l'article L. 241-2 est donnée pour une durée maximum de quatre mois. Elle cesse de plein droit de produire

effet à l'expiration de ce délai. Elle ne peut être renouvelée que dans les mêmes conditions de forme et de durée.

Article L. 242-4

Il est établi, sous l'autorité du Premier ministre, un relevé de chacune des opérations d'interception et d'enregistrement. Ce relevé mentionne la date et l'heure auxquelles elle a commencé et celles auxquelles elle s'est terminée.

Article L. 242-5

Dans les correspondances interceptées, seuls les renseignements en relation avec l'un des objectifs énumérés à l'article L. 241-2 peuvent faire l'objet d'une transcription. Cette transcription est effectuée par les personnels habilités.

Article L. 242-6

L'enregistrement est détruit sous l'autorité du Premier ministre, à l'expiration d'un délai de dix jours au plus tard à compter de la date à laquelle il a été effectué. Il est dressé procès-verbal de cette opération.

Article L. 242-7

Les transcriptions d'interceptions doivent être détruites dès que leur conservation n'est plus indispensable à la réalisation des fins mentionnées à l'article L. 241-2. Il est dressé procès-verbal de l'opération de destruction. Les opérations mentionnées aux alinéas précédents sont effectuées sous l'autorité du Premier ministre.

Article L. 242-8

Sans préjudice de l'application du deuxième alinéa de l'article 40 du Code de procédure pénale, les renseignements recueillis ne peuvent servir à d'autres fins que celles mentionnées à l'article L. 241-2.

Article L. 242-9

Les opérations matérielles nécessaires à la mise en place des interceptions dans les locaux et installations des services ou organismes placés sous l'autorité ou la tutelle du ministre chargé des « communications électroniques » ou des exploitants de réseaux ou fournisseurs de services de télécommunications ne peuvent être effectuées que sur ordre du ministre chargé des « communications électroniques » ou sur ordre de la personne spécialement déléguée par lui, par des agents qualifiés de ces services, organismes, exploitants ou fournisseurs, dans leurs installations respectives.

Chapitre III : Commission nationale de contrôle des interceptions de sécurité

Section 1 : Composition et fonctionnement

Article L. 243-1

La Commission nationale de contrôle des interceptions de sécurité est une autorité administrative indépendante chargée de veiller au respect des dispositions du présent titre.

Article L. 243-2

La Commission nationale de contrôle des interceptions de sécurité est présidée par une personnalité désignée, pour une durée de six ans, par le Président de la République, sur une liste de quatre noms établie conjointement par le vice-président du Conseil d'État et le premier président de la Cour de cassation.

Elle comprend, en outre, un député désigné pour la durée de la législature par le président de l'Assemblée nationale et un sénateur désigné après chaque renouvellement partiel du Sénat par le président du Sénat.

La qualité de membre de la Commission est incompatible avec celle de membre du Gouvernement.

Article L. 243-3

Sauf démission, il ne peut être mis fin aux fonctions de membre de la Commission qu'en cas d'empêchement constaté par celle-ci. Le mandat des membres de la Commission n'est pas renouvelable. Les membres de la Commission désignés en remplacement de ceux dont les fonctions ont pris fin avant leur terme normal achèvent le mandat de ceux qu'ils remplacent. À l'expiration de ce mandat, par dérogation au précédent alinéa, ils peuvent être nommés comme membre de la Commission s'ils ont occupé ces fonctions de remplacement pendant moins de deux ans.

Article L. 243-4

Les membres de la Commission sont astreints au respect des secrets protégés par les articles 413-10, 226-13 et 226-14 du Code pénal pour les faits, actes ou renseignements dont ils ont pu avoir connaissance en raison de leurs fonctions.

Article L. 243-5

La Commission établit son règlement intérieur. En cas de partage des voix, la voix du président est prépondérante. Les agents de la Commission sont nommés par le président.

Article L. 243-6

La Commission dispose des crédits nécessaires à l'accomplissement de sa mission dans les conditions fixées par la loi de finances. Le président est ordonnateur des dépenses de la Commission.

Article L. 243-7

La Commission remet chaque année au Premier ministre un rapport sur les conditions d'exercice et les résultats de son activité, qui précise notamment le nombre de recommandations qu'elle a adressées au Premier ministre en application de l'article L. 243-8 et au ministre de l'Intérieur en application de l'article L. 34-1-1 du Code des postes et des communications électroniques et de l'article 6 de la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, ainsi que les suites qui leur ont été données. Ce rapport est rendu public. La Commission adresse, à tout moment, au Premier ministre les observations qu'elle juge utiles.

Section 2 : Missions

Article L. 243-8

La décision motivée du Premier ministre mentionnée à l'article L. 242-1 est communiquée dans un délai de 48 heures au plus tard au président de la Commission nationale de contrôle des interceptions de sécurité. Si celui-ci estime que la légalité de cette décision au regard des dispositions du présent titre n'est pas certaine, il réunit la Commission, qui statue dans les sept jours suivant la réception par son président de la communication mentionnée au premier alinéa. Au cas où la Commission estime qu'une interception de sécurité a été autorisée en méconnaissance des dispositions du présent titre, elle adresse au Premier ministre une recommandation tendant à ce que cette interception soit interrompue. Elle porte également cette recommandation à la connaissance du ministre ayant proposé l'interception et du ministre chargé des « communications électroniques ». La Commission peut adresser au Premier ministre une recommandation, relative au contingent et à sa répartition, mentionnée à l'article L. 242-2. Le Premier ministre informe sans délai la Commission des suites données à ses recommandations.

Article L. 243-9

De sa propre initiative ou sur réclamation de toute personne y ayant un intérêt direct et personnel, la commission peut procéder au contrôle de toute interception de sécurité en vue de vérifier si elle est effectuée dans le respect des dispositions du présent titre. Si la Commission estime qu'une interception de sécurité est effectuée en violation des dispositions du présent titre, elle adresse au Premier ministre une recommandation tendant à ce que cette interception soit interrompue. Il est alors procédé ainsi qu'il est indiqué aux quatrième et sixième alinéas de l'article L. 243-8.

Article L. 243-10

Les ministres, les autorités publiques, les agents publics doivent prendre toutes mesures utiles pour faciliter l'action de la Commission.

Article L. 243-11

Lorsque la Commission a exercé son contrôle à la suite d'une réclamation, il est notifié à l'auteur de la réclamation qu'il a été procédé aux vérifications nécessaires. Conformément au deuxième alinéa de l'article 40 du Code de procédure pénale, la Commission donne avis sans délai au procureur de la République de toute infraction aux dispositions du présent titre dont elle a pu avoir connaissance à l'occasion du contrôle effectué en application de l'article L. 243-9.

Article L. 243-12

La Commission nationale de contrôle des interceptions de sécurité exerce les attributions définies à l'article L. 34-1-1 du Code des postes et des communications électroniques et à l'article 6 de la loi no 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique en ce qui concerne les demandes de communication de données formulées auprès des opérateurs de communications électroniques et personnes mentionnées à l'article L. 34-1 du code précité ainsi que des prestataires mentionnés aux 1 et 2 du I de l'article 6 de la loi no 2004-575 du 21 juin 2004 précitée.

Chapitre IV : Obligations des opérateurs et prestataires de services

Article L. 244-1

Les personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité sont tenues de remettre aux agents autorisés dans les conditions prévues à l'article L. 242-1, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies. Les agents autorisés peuvent demander aux fournisseurs de prestations susmentionnés de mettre eux-mêmes en œuvre ces conventions, sauf si ceux-ci démontrent qu'ils ne sont pas en mesure de satisfaire à ces réquisitions.

Un décret en Conseil d'État précise les procédures suivant lesquelles cette obligation est mise en œuvre ainsi que les conditions dans lesquelles la prise en charge financière de cette mise en œuvre est assurée par l'État.

Article L. 244-2

Les juridictions compétentes pour ordonner des interceptions en application du Code de procédure pénale ainsi que le Premier ministre ou, en ce qui concerne l'exécution des mesures prévues à l'article L. 241-3, le ministre de la Défense ou le ministre de l'Intérieur peuvent recueillir, auprès des personnes physiques ou morales exploitant des réseaux de communications électroniques ou fournisseurs de services de communications électroniques, les informations ou documents qui leur sont nécessaires, chacun en ce qui le concerne, pour la réalisation et l'exploitation des interceptions autorisées par la loi. La fourniture des informations ou

documents visés à l'alinéa précédent ne constitue pas un détournement de leur finalité au sens de l'article 226-21 du Code pénal.

Article L. 244-3

Dans le cadre des attributions qui lui sont conférées par le Livre II du Code des postes et des communications électroniques, le ministre chargé des « communications électroniques » veille notamment à ce que l'exploitant public, les autres exploitants de réseaux publics de communications électroniques et les autres fournisseurs de services de communications électroniques autorisés prennent les mesures nécessaires pour assurer l'application des dispositions du présent titre et de la section 3 du chapitre Ier du Titre III du Livre Ier du Code de procédure pénale relatives aux interceptions de correspondances émises par la voie des télécommunications ordonnées par l'autorité judiciaire.

Chapitre V : Dispositions pénales

Article L. 245-1

Le fait par une personne concourant, dans les cas prévus par la loi, à l'exécution d'une décision d'interception de sécurité, de révéler l'existence de l'interception est puni des peines mentionnées aux articles 226-13, 226-14 et 226-31 du Code pénal.

Article L. 245-2

Le fait de ne pas déférer, dans les conditions prévues au premier alinéa de l'article L. 244-1, aux demandes des autorités habilitées est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.

Article L. 245-3

Le fait par une personne exploitant un réseau de communications électroniques ou fournissant des services de communications électroniques de refuser, en violation du premier alinéa de l'article L. 244-2, de communiquer les informations ou documents ou de communiquer des renseignements erronés est puni de six mois d'emprisonnement et de 7 500 euros d'amende.

1.3. Les textes réglementaires récents visant la loi du 10 juillet 1991

Décret nº 2002-497 du 12 avril 2002 relatif au groupement interministériel de contrôle (*JO* du 13 avril 2002)

« […] Vu la loi nº 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des "communications électroniques", modifiée par la loi nº 92-1336 du 16 décembre 1992, l'ordonnance nº 2000-916 du 19 septembre 2000 et la loi nº 2001-1062 du 15 novembre 2001 […]. »

Article 1er – « Le groupement interministériel de contrôle est un service du Premier ministre chargé des interceptions de sécurité. »

Article 2 – « Le groupement interministériel de contrôle a pour mission :
1) de soumettre au Premier ministre les propositions d'interception présentées dans les conditions fixées par l'article 4 de la loi du 10 juillet 1991 susvisée ;
2) d'assurer la centralisation de l'exécution des interceptions de sécurité autorisées ;
3) de veiller à l'établissement du relevé d'opération prévu par l'article 8 de la loi du 10 juillet 1991 susvisée, ainsi qu'à la destruction des enregistrements effectués, dans les conditions fixées par l'article 9 de la même loi. »

Article 3 – « Le directeur du groupement interministériel de contrôle est nommé par arrêté du Premier ministre. »

Article 4 – « Le ministre de la Fonction publique et de la Réforme de l'État est chargé de l'exécution du présent décret, qui sera publié au *Journal officiel de la République française*. »

Décret nº 2002-997 du 16 juillet 2002 relatif à l'obligation mise à la charge des fournisseurs de prestations de cryptologie en application de l'article 11-1 de la loi nº 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des « communications électroniques » (*JO* du 18 juillet 2002)

Article 1 – « L'obligation mise à la charge des fournisseurs de prestations de cryptologie par l'article 11-1 de la loi du 10 juillet 1991 susvisée résulte d'une décision écrite et motivée, émanant du Premier ministre, ou de l'une des deux personnes spécialement déléguées par lui en application des dispositions de l'article 4 de la même loi.

La décision qui suspend cette obligation est prise dans les mêmes formes. »

Article 2 – « Les décisions prises en application de l'article 1er sont notifiées au fournisseur de prestations de cryptologie et communiquées sans délai au président de la Commission nationale de contrôle des interceptions de sécurité. »

Article 3 – « Les conventions mentionnées dans le présent décret permettant le déchiffrement des données s'entendent des clés cryptographiques ainsi que de tout moyen logiciel ou de toute autre information permettant la mise au clair de ces données. »

Article 4 – « La décision mentionnée au premier alinéa de l'article 1er :
a) indique la qualité des agents habilités à demander au fournisseur de prestations de cryptologie la mise en œuvre ou la remise des conventions, ainsi que les modalités selon lesquelles les données à déchiffrer lui sont, le cas échéant, transmises ;
b) fixe le délai dans lequel les opérations doivent être réalisées, les modalités selon lesquelles, dès leur achèvement, le fournisseur remet

aux agents visés au a) du présent article les résultats obtenus ainsi que les pièces qui lui ont été éventuellement transmises ;
c) prévoit, dès qu'il apparaît que les opérations sont techniquement impossibles, que le fournisseur remet aux agents visés au a) les pièces qui lui ont été éventuellement transmises. »

Article 5 – « Les fournisseurs prennent toutes dispositions, notamment d'ordre contractuel, afin que soit respectée la confidentialité des informations dont ils ont connaissance relativement à la mise en œuvre ou à la remise de ces conventions. »

Article 6 – « L'intégralité des frais liés à la mise en œuvre de l'obligation prévue par l'article 11-1 de la loi du 10 juillet 1991 susvisée est prise en charge, sur la base des frais réellement exposés par le fournisseur et dûment justifiés par celui-ci, par le budget des services du Premier ministre. »

Article 7 – « Le présent décret est applicable en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna. »

Article 8 – « Le ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales, la ministre de la Défense, le ministre de l'Économie, des Finances et de l'Industrie, la ministre de l'Outre-mer et le ministre délégué au Budget et à la Réforme budgétaire sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel de la République française*. »

Deuxième mission : les opérations de recueil de données techniques de communications

Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers

Au sein de ce texte, l'article 6 concerne directement la Commission :

Article 6

I. – Après l'article L. 34-1 du Code des postes et des communications électroniques, il est inséré un article L. 34-1-1 ainsi rédigé :

Article L. 34-1-1 – « Afin de prévenir [Dispositions déclarées non conformes à la Constitution par la décision du Conseil constitutionnel n° 2005-532 DC du 19 janvier 2006] les actes de terrorisme, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions peuvent exiger des opérateurs et personnes mentionnés au I de l'article L. 34-1 la communication des données conservées et traitées par ces derniers en application dudit article.

Les données pouvant faire l'objet de cette demande sont limitées aux données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications.

Les surcoûts identifiables et spécifiques éventuellement exposés par les opérateurs et personnes mentionnés au premier alinéa pour répondre à ces demandes font l'objet d'une compensation financière.

Les demandes des agents sont motivées et soumises à la décision d'une personnalité qualifiée, placée auprès du ministre de l'Intérieur. Cette personnalité est désignée pour une durée de trois ans renouvelable par la Commission nationale de contrôle des interceptions de sécurité sur proposition du ministre de l'Intérieur qui lui présente une liste d'au moins trois noms. Des adjoints pouvant la suppléer sont désignés dans les mêmes conditions. La personnalité qualifiée établit un rapport d'activité annuel adressé à la Commission nationale de contrôle des interceptions de sécurité. Les demandes, accompagnées de leur motif, font l'objet d'un enregistrement et sont communiquées à la Commission nationale de contrôle des interceptions de sécurité.

Cette instance peut à tout moment procéder à des contrôles relatifs aux opérations de communication des données techniques. Lorsqu'elle constate un manquement aux règles définies par le présent article ou une atteinte aux droits et libertés, elle saisit le ministre de l'Intérieur d'une recommandation. Celui-ci lui fait connaître dans un délai de quinze jours les mesures qu'il a prises pour remédier aux manquements constatés. Les modalités d'application des dispositions du présent article sont fixées par décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés et de la Commission nationale de contrôle des interceptions de sécurité, qui précise notamment la procédure de suivi des demandes et les conditions et durée de conservation des données transmises. »

II. – Après le II de l'article 6 de la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, il est inséré un II bis ainsi rédigé :

II bis – « Afin de prévenir [Dispositions déclarées non conformes à la Constitution par la décision du Conseil constitutionnel nº 2005-532 DC du 19 janvier 2006] les actes de terrorisme, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions peuvent exiger des prestataires mentionnés aux 1 et 2 du I la communication des données conservées et traitées par ces derniers en application du présent article.

Les demandes des agents sont motivées et soumises à la décision de la personnalité qualifiée instituée par l'article L. 34-1-1 du Code des postes et des communications électroniques selon les modalités prévues par le même article. La Commission nationale de contrôle des interceptions de sécurité exerce son contrôle selon les modalités prévues par ce même article.

Les modalités d'application des dispositions du présent II bis sont fixées par décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés et de la Commission nationale de contrôle des interceptions de sécurité, qui précise notamment la procédure de suivi des demandes et les conditions et durée de conservation des données transmises. »

III. – 1. À la fin de la seconde phrase du premier alinéa de l'article 4 de la loi nº 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, les mots : « Ou de la personne que chacun d'eux aura spécialement déléguée » sont remplacés par les mots : « Ou de l'une des deux personnes que chacun d'eux aura spécialement déléguées ».

2. Dans la première phrase du premier alinéa de l'article 19 de la même loi, les mots : « De l'article 14 et » sont remplacés par les mots : « De l'article 14 de la présente loi et au ministre de l'Intérieur en application de l'article L. 34-1-1 du Code des postes et des communications électroniques et de l'article 6 de la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, ainsi que ».

3. La même loi est complétée par un Titre V intitulé : « Dispositions finales » comprenant l'article 27 qui devient l'article 28.

4. Il est inséré, dans la même loi, un Titre IV ainsi rédigé :
Titre IV (de la loi nº 91-646 du 10 juillet 1991 consolidée) :
COMMUNICATION DES DONNÉES TECHNIQUES RELATIVES À DES COMMUNICATIONS ÉLECTRONIQUES

Article 27 – « La Commission nationale de contrôle des interceptions de sécurité exerce les attributions définies à l'article L. 34-1-1 du Code des postes et des communications électroniques et à l'article 6 de la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique en ce qui concerne les demandes de communication de données formulées auprès des opérateurs de communications électroniques et personnes mentionnées à l'article L. 34-1 du code précité ainsi que des prestataires mentionnés aux 1 et 2 du I de l'article 6 de la loi nº 2004-575 du 21 juin 2004 précitée. »

Cet article appelle les commentaires suivants :

– sur la « personnalité qualifiée » :

Les demandes relatives à ces données sont soumises à l'appréciation d'une personnalité qualifiée désignée par la Commission pour une durée de trois ans renouvelable, à partir d'une liste de trois noms proposée par le ministre de l'Intérieur. La même procédure est prévue pour la désignation des adjoints de cette personnalité.

– sur le champ d'application de cet article :

Le Conseil constitutionnel a censuré au nom du principe de séparation des pouvoirs la disposition liminaire de l'article 6 consistant non seulement à prévenir mais également à réprimer le terrorisme (décision no 2002-532 DC du 19 janvier 2006). Cette séparation entre réquisitions judiciaires (*cf.* notamment article 77-1-1 du Code de procédure pénale) et réquisitions administratives (articles 22 de la loi du 10 juillet 1991 et 6 de la loi no 2006-64 du 23 janvier 2006) est ainsi conforme à celle entre interceptions judiciaires (article 100 à 100-7 du Code de procédure pénale) et interceptions administratives rappelée régulièrement par la CNCIS dans ses avis et rapports publics (3e rapport 1994, p. 19 ; 7e rapport 1998, p. 23 ; 8e rapport 1999, p. 14).

Loi no 2008-1245 du 1er décembre 2008 visant à prolonger l'application des articles 3, 6 et 9 de la loi no 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

Article unique

Les dispositions des articles 3, 6 et 9 sont applicables jusqu'au 31 décembre 2012.

Le Gouvernement remet chaque année au Parlement un rapport sur l'application de la présente loi.

Le texte définitivement adopté stipule que par parallélisme avec les procédures de demandes d'interceptions, les demandes soumises à la Commission seront enregistrées, accompagnées de leur motivation et communiquées à la Commission. Le décret du 22 décembre 2006 précise que celle-ci peut à tout moment avoir accès aux données enregistrées et demander des éclaircissements sur la motivation des demandes.

Loi no 2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme (voir chapitre 2 « Actualité législative et réglementaire ») ;

Décret nº 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne

CHAPITRE I : DISPOSITIONS RELATIVES AUX RÉQUISITIONS JUDICIAIRES PRÉVUES PAR LE II DE L'ARTICLE 6 DE LA LOI Nº 2004575 DU 21 JUIN 2004

Article 1

Les données mentionnées au II de l'article 6 de la loi du 21 juin 2004 susvisée, que les personnes sont tenues de conserver en vertu de cette disposition, sont les suivantes : 1° Pour les personnes mentionnées au 1 du I du même article et pour chaque connexion de leurs abonnés :
a) l'identifiant de la connexion ;
b) l'identifiant attribué par ces personnes à l'abonné ;
c) l'identifiant du terminal utilisé pour la connexion lorsqu'elles y ont accès ;
d) les dates et heure de début et de fin de la connexion ;
e) les caractéristiques de la ligne de l'abonné.

2° Pour les personnes mentionnées au 2 du I du même article et pour chaque opération de création :
a) l'identifiant de la connexion à l'origine de la communication ;
b) l'identifiant attribué par le système d'information au contenu, objet de l'opération ;
c) les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus ;
d) la nature de l'opération ;
e) les dates et heure de l'opération ;
f) l'identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a fourni.

3° Pour les personnes mentionnées aux 1 et 2 du I du même article, les informations fournies lors de la souscription d'un contrat par un utilisateur ou lors de la création d'un compte :
a) au moment de la création du compte, l'identifiant de cette connexion ;
b) les noms et prénom ou la raison sociale ;
c) les adresses postales associées ;
d) les pseudonymes utilisés ;
e) les adresses de courrier électronique ou de compte associées ;
f) les numéros de téléphone ;
g) le mot de passe ainsi que les données permettant de le vérifier ou de le modifier, dans leur dernière version mise à jour.

4° Pour les personnes mentionnées aux 1 et 2 du I du même article, lorsque la souscription du contrat ou du compte est payante, les informations suivantes relatives au paiement, pour chaque opération de paiement :
a) le type de paiement utilisé ;

b) la référence du paiement ;
c) le montant ;
d) la date et l'heure de la transaction.

Les données mentionnées aux 3° et 4° ne doivent être conservées que dans la mesure où les personnes les collectent habituellement.

Article 2

La contribution à une création de contenu comprend les opérations portant sur :
a) des créations initiales de contenus ;
b) des modifications des contenus et de données liées aux contenus ;
c) des suppressions de contenus.

Article 3

La durée de conservation des données mentionnées à l'article 1er est d'un an :
a) s'agissant des données mentionnées aux 1° et 2°, à compter du jour de la création des contenus, pour chaque opération contribuant à la création d'un contenu telle que définie à l'article 2 ;
b) s'agissant des données mentionnées au 3°, à compter du jour de la résiliation du contrat ou de la fermeture du compte ;
c) s'agissant des données mentionnées au 4°, à compter de la date d'émission de la facture ou de l'opération de paiement, pour chaque facture ou opération de paiement.

Article 4

La conservation des données mentionnées à l'article 1er est soumise aux prescriptions de la loi du 6 janvier 1978 susvisée, notamment les prescriptions prévues à l'article 34, relatives à la sécurité des informations.

Les conditions de la conservation doivent permettre une extraction dans les meilleurs délais pour répondre à une demande des autorités judiciaires.

CHAPITRE II : DISPOSITIONS RELATIVES AUX DEMANDES ADMINISTRATIVES PRÉVUES PAR LE II BIS DE L'ARTICLE 6 DE LA LOI No 2004575 DU 21 JUIN 2004

Article 5

Les agents mentionnés au premier alinéa du II bis de l'article 6 de la loi du 21 juin 2004 susvisée sont désignés par les chefs des services de police et de gendarmerie nationales chargés des missions de prévention des actes de terrorisme, dont la liste est fixée par l'arrêté prévu à l'article 33 de la loi du 23 janvier 2006 susvisée. Ils sont habilités par le directeur général ou central dont ils relèvent.

Article 6

Les demandes de communication de données d'identification, conservées et traitées en application du II bis de l'article 6 de la loi du 21 juin 2004 susvisée, comportent les informations suivantes :
a) le nom, le prénom et la qualité du demandeur, ainsi que son service d'affectation et l'adresse de celui-ci ;
b) la nature des données dont la communication est demandée et, le cas échéant, la période intéressée ;
c) la motivation de la demande.

Article 7

Les demandes sont transmises à la personnalité qualifiée instituée à l'article L. 34-1-1 du Code des postes et des communications électroniques.

Ces demandes ainsi que les décisions de la personnalité qualifiée sont enregistrées et conservées pendant une durée maximale d'un an dans un traitement automatisé mis en œuvre par le ministère de l'Intérieur.

Article 8

Les demandes approuvées par la personnalité qualifiée sont adressées, sans les éléments mentionnés aux a et c de l'article 6, par un agent désigné dans les conditions prévues à l'article 5 aux personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi du 21 juin 2004 susvisée, lesquelles transmettent sans délai les données demandées à l'auteur de la demande.

Les transmissions prévues à l'alinéa précédent sont effectuées selon des modalités assurant leur sécurité, leur intégrité et leur suivi, définies par une convention conclue avec le prestataire concerné ou, à défaut, par un arrêté conjoint du ministre de l'Intérieur et du ministre chargé de l'Industrie.

Les données fournies par les personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi du 21 juin 2004 susvisée sont enregistrées et conservées pendant une durée maximale de trois ans dans des traitements automatisés mis en œuvre par le ministère de l'Intérieur et le ministère de la Défense.

Article 9

Une copie de chaque demande est transmise, dans un délai de sept jours à compter de l'approbation de la personnalité qualifiée, à la Commission nationale de contrôle des interceptions de sécurité. Un arrêté du ministre de l'Intérieur, pris après avis de celle-ci, définit les modalités de cette transmission.

La Commission peut, en outre, à tout moment, avoir accès aux données enregistrées dans les traitements automatisés mentionnés aux

articles 7 et 8. Elle peut également demander des éclaircissements sur la motivation des demandes approuvées par la personnalité qualifiée.

Article 10

Les surcoûts identifiables et spécifiques supportés par les personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi du 21 juin 2004 susvisée pour la fourniture des données prévue par l'article II bis du même article font l'objet d'un remboursement par l'État par référence aux tarifs et selon des modalités fixés par un arrêté conjoint du ministre de l'Intérieur et du ministre chargé du Budget.

CHAPITRE III : DISPOSITIONS DIVERSES

Article 11

À l'article R. 10-19 du Code des postes et des communications électroniques, les mots : « sans leur motivation » sont remplacés par les mots : « Sans les éléments mentionnés aux a et c de l'article R. 10-17 ».

Article 12

Les dispositions du présent décret sont applicables sur tout le territoire de la République à l'exception des dispositions des articles 1er à 4, 10 et 11 qui ne sont pas applicables dans les Terres australes et antarctiques françaises.

Article 13

Le garde des Sceaux, ministre de la Justice et des Libertés, le ministre de l'Intérieur, de l'Outre-mer, des Collectivités territoriales et de l'Immigration, la ministre de l'Économie, des Finances et de l'Industrie et le ministre du Budget, des Comptes publics, de la Fonction publique et de la Réforme de l'État, porte-parole du Gouvernement, sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel de la République française.*

Troisième mission : le contrôle des matériels d'interception

Cette activité de « contrôle du matériel » s'inscrit dans un cadre juridique qu'il convient de rappeler ici :

• Les dispositions législatives qui définissent et répriment les infractions d'atteinte à la vie privée et au secret des correspondances :
– article 226-1 du Code pénal : réprimant les atteintes à la vie privée ;
– article 226-15 du Code pénal : réprimant le détournement de correspondance.

Ce texte inclut, dans cette notion de détournement, le fait, de mauvaise foi : « D'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions » ;
– article 226-3 du Code pénal : réprimant la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente, en l'absence d'autorisation ministérielle dont les conditions sont fixées par décret en Conseil d'État, d'appareils conçus pour réaliser les opérations pouvant constituer l'infraction prévue par l'article 226-15 du Code pénal.

• **Le décret 97-757 du 10 juillet 1997** qui met en œuvre, à la faveur des articles R. 226-1 à R. 226-12 du Code pénal, la procédure d'« autorisation ministérielle » prévue par l'article 226-3 du Code pénal. L'organisation de la Commission consultative placée sous la présidence du directeur général de l'Agence nationale de sécurité des systèmes d'information, pièce de la procédure d'autorisation est décrite par ce dispositif (article R. 226-2 du Code pénal).

• **Les dispositions réglementaires portant sur l'organisation et le fonctionnement des entités chargées de l'examen des demandes des services de l'État et des sociétés privées :**

• Le décret 2009-619 du 6 juin 2009 relatif à certaines commissions administratives à caractère consultatif relevant du Premier ministre ;

• Le décret 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information » : ce texte confie la Présidence de la Commission dite « R 226 » au directeur général de l'Agence nationale de la sécurité, lui-même rattaché au Secrétariat général de la défense et de la sécurité nationale :
– article 4 : l'Agence nationale de la sécurité des systèmes d'information se prononce sur la sécurité des dispositifs et des services, offerts par les prestataires, nécessaires à la protection des systèmes d'information.

L' Agence est en particulier chargée, par délégation du Premier ministre :
– de la certification de sécurité des dispositifs de création et de vérification de signature électronique prévue par le décret du 30 mars 2001 susvisé ;
– de l'agrément des centres d'évaluation et de la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information prévus par le décret du 18 avril 2002 susvisé ;
– de la délivrance des autorisations et de la gestion des déclarations relatives aux moyens et aux prestations de cryptologie prévues par le décret du 2 mai 2007 susvisé.

L' Agence instruit les demandes d'autorisation présentées en application de l'article 226-3 du Code pénal.

• Le décret 2009-1657 du 24 décembre 2009 relatif au conseil de défense et de sécurité nationale et au secrétariat général de la défense et de la sécurité nationale :
– article 5.
– – I. : À l'article 2 du décret du 7 juillet 2009 susvisé, la référence : « l'article D. 1132-10 » est remplacée par la référence « le 7° de l'article R. 1132-3 ».
– – II. : Dans les articles R. 226-2, R. 226-4 et R. 226-8 du Code pénal, les mots : « Le secrétariat général de la défense nationale » sont remplacés par les mots : « l'Agence nationale de la sécurité des systèmes d'information ».
– – III. : Dans toutes les dispositions à caractère réglementaire, sous réserve des dispositions du II du présent article, les références au conseil de défense, au Secrétariat général de la défense nationale et au secrétaire général de la défense nationale sont remplacés respectivement par les références au conseil de défense et de sécurité nationale, au Secrétariat général de la défense et de la sécurité nationale et au Secrétaire général de la défense et de la sécurité nationale.

• Le décret no 2011-1431 du 3 novembre 2011 portant modification du Code de procédure pénale (partie réglementaire : Décrets simples) pris pour l'application de l'article 706-102-6 de ce code relatif à la captation des données informatiques.

Article 1

Il est ajouté au chapitre Ier du Titre Ier du Livre Ier du Code de procédure pénale (partie réglementaire : Décrets simples) une section 5 ainsi rédigée :

« Section 5

De la captation des données informatiques

Art. D. 15-1-6.-Les services, unités et organismes, visés à l'article 706-102-6, pouvant procéder aux opérations d'installation des dispositifs techniques mentionnés à l'article 706-102-1 sont :

• la Direction centrale de la police judiciaire et ses directions interrégionales et régionales ;
• la Direction centrale du renseignement intérieur ;
• les offices centraux de police judiciaire ;
• l'Unité de recherche, assistance, intervention et dissuasion ;
• les groupes d'intervention de la Police nationale ;
• la sous-direction de la police judiciaire de la Gendarmerie nationale ;
• les sections de recherches de la Gendarmerie nationale ;
• les sections d'appui judiciaire de la Gendarmerie nationale ;
• le groupe d'intervention de la Gendarmerie nationale. »

Article 2

Le garde des Sceaux, ministre de la Justice et des Libertés, et le ministre de l'Intérieur, de l'Outre-mer, des Collectivités territoriales et de l'Immigration sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel de la République française.*

• L'arrêté du 29 juillet 2004 (*cf.* rapport d'activité 2004, p. 35-38) fixant la liste des appareils soumis à autorisation ministérielle pour application de l'article 226-3 du Code pénal, abrogé et remplacé par l'arrêté du 4 juillet 2012 (*cf.* chapitre 2 « Actualité législative et réglementaire ») ;

• L'arrêté du 16 août 2006 mettant en œuvrant de manière spécifique le régime relatif au « registre » prévu par l'article R. 226-10 du Code pénal (registre retraçant la gestion des matériels soumis à autorisation). Cet arrêté a emporté l'abrogation de l'arrêté du 15 janvier 1998 qui constituait jusqu'alors le siège de cette matière ;

• L'instruction du 5 septembre 2006, véritable documentation pédagogique à l'attention des « usagers » de la réglementation relative au matériel. Elle constitue un guide pratique efficace offrant une présentation claire des modalités procédurales d'examen des demandes, ainsi que des règles de compétence de la Commission consultative dite « R 226 ».

Chapitre II

Actualité législative et réglementaire

1) Loi nº 2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme

NOR : INTX1232040L

JORF nº 0298 du 22 décembre 2012

L' Assemblée nationale et le Sénat ont adopté,

Le Président de la République promulgue la loi dont la teneur suit :

Article 1

À la fin du dernier alinéa de l'article L. 222-1 du Code de la sécurité intérieure et du premier alinéa de l'article 32 de la loi nº 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, l'année : « 2012 » est remplacée par l'année : « 2015 ».

Article 2

La section 2 du chapitre III du Titre Ier du Livre Ier du Code pénal est complétée par un article 113-13 ainsi rédigé :

« Art. 113-13.- La loi pénale française s'applique aux crimes et délits qualifiés d'actes de terrorisme et réprimés par le Titre II du Livre IV commis à l'étranger par un Français ou par une personne résidant habituellement sur le territoire français. »

Article 3

Après l'article 421-2-3 du même code, il est inséré un article 421-2-4 ainsi rédigé :

« Art. 421-2-4.- Le fait d'adresser à une personne des offres ou des promesses, de lui proposer des dons, présents ou avantages quelconques, de la menacer ou d'exercer sur elle des pressions afin qu'elle participe à un groupement ou une entente prévu à l'article 421-2-1 ou qu'elle commette un des actes de terrorisme mentionnés aux articles 421-1 et 421-2 est puni, même lorsqu'il n'a pas été suivi d'effet, de dix ans d'emprisonnement et de 150 000 euros d'amende. »

Article 4

La loi du 29 juillet 1881 sur la liberté de la presse est ainsi modifiée :

1° Après le mot : « Être », la fin de l'article 52 est ainsi rédigée : « Placée en détention provisoire que dans les cas prévus à l'article 23 et aux deuxième à quatrième et sixième alinéas de l'article 24 » ;

2° À l'article 65-3, la référence : « Le huitième alinéa » est remplacée par les références : « Les sixième et huitième alinéas ».

Article 5

Le IV de l'article 9 de la loi no 86-1020 du 9 septembre 1986 relative à la lutte contre le terrorisme est complété par deux alinéas ainsi rédigés :

« Si des poursuites pénales ont été engagées, ce droit d'action peut également être exercé dans un délai d'un an à compter de la décision de la juridiction qui a statué définitivement sur l'action publique ou sur l'action civile engagée devant la juridiction répressive. Lorsque l'auteur de l'infraction est condamné à verser des dommages et intérêts, la juridiction doit informer la partie civile de sa possibilité de saisir le fonds et le délai d'un an ne court qu'à compter de cette information.

« Dans tous les cas, le conseil d'administration du fonds peut relever le requérant de la forclusion résultant de l'application des deuxième et troisième alinéas du présent IV si celui-ci n'a pas été en mesure de faire valoir ses droits dans les délais requis ou pour tout autre motif légitime. »

Article 6

À la première phrase de l'article L. 562-1 du Code monétaire et financier, après les mots : « Contre le terrorisme, », sont insérés les mots : « y incitent, ».

Article 7

À l'article L. 562-6 du même code, après le mot : « Publiées », sont insérés les mots : « Par extrait ».

Article 8

I. La première phrase du premier alinéa de l'article L. 562-8 du même code est ainsi modifiée :

1° Après le mot : « Chargés », sont insérés les mots : « De préparer et » ;

2° Sont ajoutés les mots : « Et de surveiller les opérations portant sur les fonds, les instruments financiers et les ressources économiques desdites personnes ».

II. Le II de l'article L. 561-29 du même code est complété par un alinéa ainsi rédigé :

« Le service peut également transmettre aux services de l'État chargés de préparer et de mettre en œuvre une mesure de gel ou d'interdiction de mouvement ou de transfert des fonds, des instruments financiers et des ressources économiques, des informations en relation avec l'exercice de leur mission. »

Article 9

I. L'article L. 522-2 du Code de l'entrée et du séjour des étrangers et du droit d'asile est complété par un alinéa ainsi rédigé :

« La Commission rend son avis dans le délai d'un mois à compter de la remise à l'étranger de la convocation mentionnée au premier alinéa. Toutefois, lorsque l'étranger demande le renvoi pour un motif légitime, la commission prolonge ce délai, dans la limite d'un mois maximum à compter de la décision accordant ce renvoi. À l'issue du délai d'un mois ou, si la Commission l'a prolongé, du délai supplémentaire qu'elle a fixé, les formalités de consultation de la Commission sont réputées remplies. »

II. Après le dixième alinéa de l'article 32 des ordonnances n° 2000-371 du 26 avril 2000 relative aux conditions d'entrée et de séjour des étrangers dans les îles Wallis et Futuna et n° 2000-373 du 26 avril 2000 relative aux conditions d'entrée et de séjour des étrangers à Mayotte, il est inséré un alinéa ainsi rédigé :

« La Commission rend son avis dans le délai d'un mois à compter de la remise à l'étranger de la convocation mentionnée au huitième alinéa. Toutefois, lorsque l'étranger demande le renvoi pour un motif légitime, la commission prolonge ce délai, dans la limite d'un mois maximum à compter de la décision accordant ce renvoi. À l'issue du délai d'un mois ou, si la commission l'a prolongé, du délai supplémentaire qu'elle a fixé, les formalités de consultation de la commission sont réputées remplies. »

III. L'article 34 des ordonnances n° 2000-372 du 26 avril 2000 relative aux conditions d'entrée et de séjour des étrangers en Polynésie française et n° 2002-388 du 20 mars 2002 relative aux conditions d'entrée et de séjour des étrangers en Nouvelle-Calédonie est complété par un alinéa ainsi rédigé :

« La Commission rend son avis dans le délai d'un mois à compter de la remise à l'étranger de la convocation mentionnée au huitième alinéa. Toutefois, lorsque l'étranger demande le renvoi pour un motif légitime, la Commission prolonge ce délai, dans la limite d'un mois maximum à compter de la décision accordant ce renvoi. À l'issue du délai d'un mois ou, si la commission l'a prolongé, du délai supplémentaire qu'elle a fixé, les formalités de consultation de la Commission sont réputées remplies. »

Article 10

I. Au deuxième alinéa de l'article L. 624-4 du Code de l'entrée et du séjour des étrangers et du droit d'asile, la référence : « L. 561-3 » est remplacée par la référence : « L. 571-3 ».

II. Au dernier alinéa de l'article 41-1 des ordonnances nº 2000-371 et nº 2000-373 du 26 avril 2000 précitées, la référence : «Troisième alinéa » est remplacée par la référence : « Dernier alinéa ».

III. Au dernier alinéa de l'article 43-1 des ordonnances nº 2000-372 du 26 avril 2000 et nº 2002-388 du 20 mars 2002 précitées, la référence : «Troisième alinéa » est remplacée par la référence : « Cinquième alinéa ».

Article 11

I. Dans les conditions prévues à l'article 38 de la Constitution, le Gouvernement est autorisé à prendre par ordonnance les dispositions nécessaires pour modifier la partie législative du Code de la sécurité intérieure et la partie législative du Code de la défense afin d'inclure dans ces codes certaines dispositions de la loi nº 2012-304 du 6 mars 2012 relative à l'établissement d'un contrôle des armes moderne, simplifié et préventif.

Les dispositions à codifier sont celles de la loi nº 2012-304 du 6 mars 2012 précitée, sous réserve des modifications nécessaires :
1) pour assurer le respect de la hiérarchie des normes et la cohérence rédactionnelle des textes et adapter le plan des codes ;
2) pour abroger les dispositions devenues sans objet ;
3) pour étendre aux Terres australes et antarctiques françaises les dispositions prévues par la loi nº 2012-304 du 6 mars 2012 précitée.

II. Dans les conditions prévues à l'article 38 de la Constitution, le Gouvernement est autorisé à prendre par ordonnance les dispositions nécessaires pour modifier la partie législative du Code de la sécurité intérieure :
1) pour remédier, dans les dispositions relatives à l'outre-mer, aux éventuelles erreurs de codification ;
2) pour étendre, le cas échéant avec les adaptations nécessaires, certaines dispositions du Code de la sécurité intérieure à la Polynésie française, aux Terres australes et antarctiques françaises, aux îles Wallis et Futuna et à la Nouvelle-Calédonie ainsi que pour permettre les adaptations nécessaires à l'application de ces dispositions à Mayotte, à Saint-Barthélemy, à Saint-Martin et à Saint-Pierre-et-Miquelon ;

3) pour remédier aux omissions dans la liste des dispositions abrogées en raison de leur codification par l'ordonnance n° 2012-351 du 12 mars 2012 relative à la partie législative du Code de la sécurité intérieure.

III. Les ordonnances mentionnées aux I et II doivent être prises au plus tard le 1er septembre 2013.

Un projet de loi de ratification est déposé devant le Parlement dans un délai de trois mois à compter de la publication de chaque ordonnance.

Article 12

I. Après le chapitre Ier du Livre IV du Code des pensions militaires d'invalidité et des victimes de la guerre, il est inséré un chapitre Ier bis ainsi rédigé :

« Chapitre Ier bis

« Mention "Mort pour le service de la Nation"

« Art. L. 492 ter.- Le ministre compétent peut décider que la mention "Mort pour le service de la Nation" est portée sur l'acte de décès :

« 1) d'un militaire tué en service ou en raison de sa qualité de militaire ;

« 2) d'un autre agent public tué en raison de ses fonctions ou de sa qualité.

« Lorsque, pour un motif quelconque, la mention "Mort pour le service de la Nation" n'a pu être inscrite sur l'acte de décès au moment de la rédaction de celui-ci, elle est ajoutée ultérieurement dès que les éléments nécessaires de justification le permettent.

« Lorsque la mention "Mort pour le service de la Nation" a été portée sur son acte de décès dans les conditions prévues au présent article, l'inscription du nom du défunt sur un monument de sa commune de naissance ou de dernière domiciliation est obligatoire.

« La demande d'inscription est adressée au maire de la commune choisie par la famille ou, à défaut, par les autorités civiles ou militaires, les élus nationaux, les élus locaux, l'Office national des anciens combattants et victimes de guerre par l'intermédiaire de ses services départementaux ou les associations ayant intérêt à agir.

« Les enfants des personnes dont l'acte de décès porte la mention "Mort pour le service de la Nation" ont vocation à la qualité de pupille de la Nation. »

II. Le I est applicable aux décès survenus à compter du 1er janvier 2002.

III. La loi n° 86-1020 du 9 septembre 1986 relative à la lutte contre le terrorisme est ainsi modifiée :
1) l'article 9 est complété par un VI ainsi rédigé :

« VI. Le ministre de la justice peut décider, avec l'accord des ayants droit, que la mention "Victime du terrorisme" est portée sur l'acte de décès de toute personne mentionnée au I.

« Lorsque, pour un motif quelconque, la mention "Victime du terrorisme" n'a pas pu être inscrite sur l'acte de décès au moment de la rédaction de celui-ci, elle est ajoutée ultérieurement dès que les éléments nécessaires de justification le permettent.

« Les enfants des personnes dont l'acte de décès porte la mention "Victime du terrorisme" ont vocation à la qualité de pupille de la Nation » ;

2) Au II de l'article 10, après la référence : « IV », est insérée la référence : « et VI ».

Article 13

La présente loi est applicable sur l'ensemble du territoire de la République.

La présente loi sera exécutée comme loi de l'État.

Fait à Paris, le 21 décembre 2012.
François Hollande
Par le Président de la République :
Le Premier ministre,
Jean-Marc Ayrault
La garde des Sceaux,
ministre de la Justice,
Christiane Taubira
Le ministre de l'Économie et des Finances,
Pierre Moscovici
Le ministre de l'Intérieur,
Manuel Valls
Le ministre de la Défense,
Jean-Yves Le Drian
La ministre de la Réforme de l'État, de la décentralisation et de la Fonction publique,
Marylise Lebranchu
Le ministre des Outre-mer,
Victorin Lurel

(1) Travaux préparatoires : loi nº 2012-1432. Sénat : projet de loi nº 6 (2012-2013) ; rapport de M. Jacques Mézard, au nom de la Commission des lois, nº 35 (2012-2013) ; texte de la Commission nº 36 (2012-2013) ; discussion et adoption, après engagement de la procédure accélérée, le 16 octobre 2012 (TA nº 12, 2012-2013). Assemblée nationale : projet de loi, adopté par le Sénat, nº 297 ; rapport de Mme Marie-Françoise Bechtel, au nom de la Commission des lois, nº 409 ; discussion et adoption le 27 novembre 2012 (TA nº 49). Sénat : projet de loi, modifié par l'Assemblée nationale, nº 170 (2012-2013) ; rapport de M. Jacques Mézard, au nom de la Commission mixte paritaire, nº 191 (2012-2013) ; texte de la Commission nº 192 (2012-2013) ; discussion et adoption le 10 décembre 2012 (TA nº 44, 2012-2013). Assemblée nationale : rapport de Mme Marie-Françoise Bechtel, au nom de la Commission mixte paritaire, nº 478 ; discussion et adoption le 12 décembre 2012 (TA nº 64).

2) Arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du Code pénal

NOR : PRMD1230326A

Le Premier ministre,

Vu la directive 98/34/CE du Parlement européen et du Conseil du 22 juin 1998 modifiée prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information ;

Vu le Code pénal, notamment les articles 226-3, R. 226-1 et suivants ;

Vu le Code de procédure pénale, notamment les articles 706-102-1 et suivants ;

Vu l'avis de la commission consultative instituée par l'article R. 226-2 du Code pénal en date du 13 septembre 2011 ;

Vu la notification à la Commission européenne nº 2012/65/F du 1er février 2012,

Arrête :

Article 1

La liste prévue par l'article 226-3 du Code pénal des appareils et des dispositifs techniques soumis à l'autorisation mentionnée à l'article R. 226-3 de ce code figure en annexe I au présent arrêté.

Article 2

La liste prévue par l'article 226-3 du Code pénal des appareils et des dispositifs techniques soumis à l'autorisation mentionnée à l'article R. 226-7 de ce code figure en annexe II au présent arrêté.

Article 3

A modifié les dispositions suivantes :
– Abroge arrêté du 29 juillet 2004 (Ab).
– Abroge Arrêté du 29 juillet 2004 – APPAREILS SOUMIS À AUTORISATION EN APPLICATION… (Ab).
– Abroge arrêté du 29 juillet 2004 – APPAREILS SOUMIS À AUTORISATION EN APPLICATION…(Ab).
– Abroge arrêté du 29 juillet 2004 – Annexes (Ab).
– Abroge arrêté du 29 juillet 2004 – art. 1 (Ab).
– Abroge arrêté du 29 juillet 2004 – art. 2 (Ab).
– Abroge arrêté du 29 juillet 2004 – art. 3 (Ab).
– Abroge arrêté du 29 juillet 2004 – art. 4 (Ab).
– Abroge arrêté du 29 juillet 2004 – art. ANNEXE I (Ab).
– Abroge arrêté du 29 juillet 2004 – art. ANNEXE II (Ab).

Article 4

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information est chargé de l'exécution du présent arrêté, qui sera publié au *Journal officiel de la République française.*

Annexes

Article annexe I

APPAREILS ET DISPOSITIFS TECHNIQUES SOUMIS À AUTORISATION EN APPLICATION DE L'ARTICLE R. 226-3 DU CODE PÉNAL

1. Appareils, à savoir tous dispositifs matériels et logiciels, conçus pour réaliser l'interception, l'écoute, l'analyse, la retransmission, l'enregistrement ou le traitement de correspondances émises, transmises ou reçues sur des réseaux de communications électroniques, opérations pouvant constituer l'infraction prévue par le deuxième alinéa de l'article 226-15 du Code pénal.

Entrent notamment dans cette catégorie :
– les appareils dont les fonctionnalités qui participent à l'interception, l'écoute, l'analyse, la retransmission, l'enregistrement ou le traitement de correspondances ne sont pas activées, quel que soit le moyen d'activation ;
– les appareils permettant, par des techniques non intrusives d'induction électromagnétique ou de couplage optique, d'intercepter ou d'écouter les correspondances transitant sur les câbles filaires ou les câbles optiques des réseaux de communications électroniques.

N'entrent pas dans cette catégorie :
– les appareils de tests et de mesures utilisables exclusivement pour l'établissement, la mise en service, le réglage et la maintenance des réseaux et systèmes de communications électroniques ;
– les appareils conçus pour un usage grand public et permettant uniquement l'exploration manuelle ou automatique du spectre radioélectrique en vue de la réception et de l'écoute de fréquences ;
– les dispositifs permettant de réaliser l'enregistrement des communications reçues ou émises par des équipements terminaux de télécommunications, lorsque cet enregistrement fait partie des fonctionnalités prévues par les caractéristiques publiques de ces équipements.

2. Appareils qui, spécifiquement conçus pour détecter à distance les conversations afin de réaliser à l'insu du locuteur l'interception, l'écoute ou la retransmission de la parole, directement ou indirectement, par des moyens acoustiques, électromagnétiques ou optiques, permettent de réaliser l'infraction prévue par l'article 226-1 du Code pénal.

Entrent dans cette catégorie :
– les dispositifs micro-émetteurs permettant la retransmission de la voix par moyens hertziens, optiques ou filaires, à l'insu du locuteur ;
– les appareils d'interception du son à distance de type microcanon ou équipés de dispositifs d'amplification acoustique ;

– les systèmes d'écoute à distance par faisceaux laser.

3. Dispositifs techniques, à savoir tous matériels ou logiciels, spécifiquement conçus pour, sans le consentement des intéressés, accéder aux données informatiques, les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères, opérations ayant pour objet la captation de données informatiques prévue par l'article 706-102-1 du Code de procédure pénale.

N'entrent pas dans cette catégorie les dispositifs de tests et de mesures des signaux radioélectriques émis par un équipement électronique destinés exclusivement à évaluer la compatibilité ou le champ électromagnétique.

Article annexe II

APPAREILS ET DISPOSITIFS TECHNIQUES SOUMIS À AUTORISATION EN APPLICATION DE L'ARTICLE R. 226-7 DU CODE PÉNAL

1. Appareils, à savoir tous dispositifs matériels et logiciels, conçus pour réaliser l'interception, l'écoute, l'analyse, la retransmission, l'enregistrement ou le traitement de correspondances émises, transmises ou reçues sur des réseaux de communications électroniques, opérations pouvant constituer l'infraction prévue par le deuxième alinéa de l'article 226-15 du Code pénal.

Entrent notamment dans cette catégorie :
– les appareils dont les fonctionnalités qui participent à l'interception, l'écoute, l'analyse, la retransmission, l'enregistrement ou le traitement de correspondances ne sont pas activées, quel que soit le moyen d'activation ;
– les appareils permettant, par des techniques non intrusives d'induction électromagnétique ou de couplage optique, d'intercepter ou d'écouter les correspondances transitant sur les câbles filaires ou les câbles optiques des réseaux de communications électroniques.

N'entrent pas dans cette catégorie :
– les appareils de tests et de mesures acquis exclusivement pour l'établissement, la mise en service, le réglage et la maintenance des réseaux et systèmes de communications électroniques ;
– les dispositifs permettant de réaliser l'enregistrement des communications reçues ou émises par des équipements terminaux de télécommunications, lorsque cet enregistrement fait partie des fonctionnalités prévues par les caractéristiques publiques de ces équipements.

2. Appareils permettant l'analyse du spectre radioélectrique ou son exploration manuelle ou automatique en vue de la réception et de l'écoute des fréquences n'appartenant pas aux bandes de fréquences attribuées seules ou en partage par le tableau national de répartition

des bandes de fréquences au service de radiodiffusion, ou au service radioamateur, ou aux installations radioélectriques pouvant être établies librement en application de l'article L. 33-3 du Code des postes et des communications électroniques, ou aux postes émetteurs et récepteurs fonctionnant sur les canaux banalisés dits CB.

3. Appareils qui, spécifiquement conçus pour détecter à distance les conversations afin de réaliser à l'insu du locuteur l'interception, l'écoute ou la retransmission de la parole, directement ou indirectement, par des moyens acoustiques, électromagnétiques ou optiques, permettent de réaliser l'infraction prévue par l'article 226-1 du Code pénal.

Entrent dans cette catégorie :
– les dispositifs micro-émetteurs permettant la retransmission de la voix par moyens hertziens, optiques ou filaires, à l'insu du locuteur ;
– les appareils d'interception du son à distance de type microcanon ou équipés de dispositifs d'amplification acoustique ;
– les systèmes d'écoute à distance par faisceaux laser.

4. Dispositifs techniques, à savoir tous matériels ou logiciels, spécifiquement conçus pour, sans le consentement des intéressés, accéder aux données informatiques, les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères, opérations ayant pour objet la captation de données informatiques prévue par l'article 706-102-1 du Code de procédure pénale.

N'entrent pas dans cette catégorie les dispositifs de tests et de mesures des signaux radioélectriques émis par un équipement électronique, destinés exclusivement à évaluer la compatibilité ou le champ électromagnétique.

Fait le 4 juillet 2012.
Pour le Premier ministre et par délégation :
Le secrétaire général de la défense
et de la sécurité nationale,
F. Delon

Chapitre III

Jurisprudence et actualités parlementaires

Arrêt du 10 mai 2012 de la Chambre criminelle de la Cour de cassation no 11-87328

LA COUR DE CASSATION, CHAMBRE CRIMINELLE, a rendu l'arrêt suivant :

Statuant sur le pourvoi formé par :
– M. Kiril X...,

contre l'arrêt de la chambre de l'instruction de la cour d'appel de Lyon, en date du 6 septembre 2011, qui, dans l'information suivie contre lui pour proxénétisme aggravé en bande organisée, traite d'êtres humains aggravée en bande organisée, a prononcé sur sa demande d'annulation d'actes de la procédure ;

Vu l'ordonnance du président de la chambre criminelle, en date du 4 novembre 2011, prescrivant l'examen immédiat du pourvoi ;

Vu le mémoire et les observations complémentaires produits ;

[……]

« En ce que l'arrêt attaqué a rejeté la demande d'annulation des interceptions de correspondances du 19 août 2009 et des actes subséquents ;

« aux motifs que la mise en place de l'écoute a eu lieu techniquement le 6 août 2008 à 17 heures ; que, nonobstant la mention portée par son rédacteur sur le procès-verbal de la cote D121, cette autorisation ne peut entrer en vigueur qu'à compter du moment où le dispositif est mis en place, en l'espèce, le 6 août 2009, et non à compter de la date de l'ordonnance ; que, dès lors, ces écoutes ont valablement été enregistrées jusqu'au 19 août 2009 ; que le procès-verbal (Dl30) mentionne l'enregistrement d'une communication du 20 août 2009 ; que seule la transcription de l'existence de cette communication, sans mention du contenu figure à la cote D130 ; que cette mention sera annulée par cancellation ; que le conseil de M. X... sollicite, par ailleurs, l'annulation de l'ordonnance de prolongation des écoutes prises pour quinze jours à compter du 28 août, au motif que cette prolongation aurait pour fondement les écoutes du 19 août ; que le juge des libertés et de la détention était en droit, quand bien même la première période d'écoute aurait été infructueuse, d'ordonner de nouvelles écoutes sur la même ligne ; qu'elle est d'autant plus justifiée que, précisément le 19 août 2009, cette ligne s'est révélée active ; que le juge des libertés et de la détention, par ordonnance du 28 août 2009, a autorisé la poursuite des écoutes sur cette ligne, pour quinze jours ; que le dispositif a été réinstallé le même jour ; que ces écoutes ont permis de révéler le numéro de téléphone de Mme J... À..., le 2 septembre 2009 ; que cette interception est parfaitement régulière, de même que les interceptions réalisées après autorisation du juge des libertés et de la détention du 16 septembre 2009 mises en place le même jour pour quinze jours sur la ligne de cette dernière, fournissant des indications, lors de communications surprises entre le 17 et le 23 septembre sur les faits reprochés à M. X... ; qu'il n'y a lieu à annulation de ces actes ;

« 1) alors que le juge des libertés et de la détention est seul compétent, sur le fondement de l'article 706-95 du Code de procédure pénale, pour fixer la durée d'une écoute téléphonique et dès lors, en fixer le point de départ ; que, sauf indication contraire dans l'ordonnance du juge des libertés et de la détention autorisant l'interception des correspondances d'une ligne téléphonique, le point de départ de cette autorisation ne peut dès lors courir qu'à compter du jour de cette ordonnance ; qu'en l'espèce, l'ordonnance a été délivrée le 5 août 2009 pour une durée de deux semaines, soit quatorze jours, venant à expiration le 18 août 2009 ; qu'en refusant, dès lors, d'annuler les écoutes illégalement réalisées le 19 août 2009, la chambre de l'instruction a violé les textes susvisés ;

« 2) alors que le juge des libertés et de la détention ne peut renouveler une fois, dans les mêmes conditions de forme et de durée, une interception téléphonique que si les nécessités de l'enquête l'exigent ; que l'ordonnance de prolongation de l'écoute d'une ligne téléphonique dont les enquêteurs avaient constaté, comme le faisait valoir le demandeur, offre de preuve à l'appui, qu'elle n'était "visiblement pas utilisée "jusqu'au 19 août à 13 h 56, a pour support nécessaire la réactivation de la ligne constatée postérieurement, ainsi que le relève l'arrêt attaqué, qui,

seule, caractérise la nécessité, pour les besoins de l'enquête, du renouvellement de la mesure ; qu'en refusant dès lors d'annuler l'ordonnance de prolongation, ayant pour support nécessaire les écoutes illégalement réalisées les 19 et 20 août 2009, et les écoutes subséquentes, faisant grief à M. X... pour avoir été à l'origine de sa mise en cause, la chambre de l'instruction a derechef violé les textes visés au moyen » ;

Attendu qu'il résulte de l'arrêt attaqué et des pièces de la procédure que, par ordonnance en date du 5 août 2010, le juge d'instruction a ordonné l'interception de communications téléphoniques pour une durée de quatorze jours ;

Attendu que c'est donc à bon droit que la chambre de l'instruction, pour refuser de faire droit au moyen d'annulation, en ce qu'il invoquait l'irrégularité des interceptions effectuées le 19 août 2010 et de celles dont elles seraient le support, a décidé que le point de départ de ces mesures devait être fixé au jour de leur mise en place effective qui a eu lieu le lendemain de l'ordonnance du magistrat les autorisant ;

D'où il suit que le moyen n'est pas fondé ;

[……]

Arrêt du 4 février 2013 du Conseil d'État (10e et 9e sous-sections réunies) no 344266.

Vu le pourvoi, enregistré le 10 novembre 2010 au secrétariat du contentieux du Conseil d'État, présenté par le garde des Sceaux, ministre de la Justice et des Libertés ; le ministre demande au Conseil d'État :

1°) d'annuler l'arrêt no 09NC01262 du 23 septembre 2010 de la cour administrative d'appel de Nancy en tant qu'après avoir annulé le jugement du 25 juin 2009 du tribunal administratif de Strasbourg et évoqué, elle a annulé la décision du 22 mai 2008 du directeur interrégional des services pénitentiaires de Strasbourg confirmant la sanction disciplinaire infligée à M. À...B... ;

[……]

1. Considérant qu'il ressort des pièces du dossier soumis aux juges du fond que, par décision du 22 mai 2008, le directeur interrégional des services pénitentiaires de Strasbourg a confirmé la sanction de placement en cellule disciplinaire pour une durée de trente jours infligée à M. B..., détenu à...,; qu'après avoir annulé le jugement du 25 juin 2009 par lequel le tribunal administratif de Strasbourg, s'estimant saisi d'un recours de plein contentieux, avait réformé cette décision, la cour administrative d'appel de Nancy a, par l'arrêt attaqué du 23 septembre 2010, annulé cette sanction ;

2. Considérant que les dispositions des articles D. 249-1 à D. 249-3 du Code de procédure pénale, alors en vigueur, classent les fautes disciplinaires pouvant être reprochées aux détenus selon trois degrés de gravité ; que constitue notamment, aux termes du 3° de l'article D. 249-1, une faute du premier degré le fait « de détenir des stupéfiants ou tous objets ou substances dangereux pour la sécurité des personnes et de l'établissement ou de faire trafic de tels objets ou substances » ; que ces mêmes faits, s'ils concernent des objets ou substances non autorisés mais non dangereux, constituent, en application du 9° de l'article D. 249-2, une faute du deuxième degré ; qu'enfin, il résulte des dispositions des articles D. 251 et D. 251-3 du même code, applicables au litige, que si, pour les détenus majeurs, la mise en cellule disciplinaire peut être infligée pour toute faute disciplinaire, sa durée ne peut excéder quarante-cinq jours pour une faute du premier degré, trente jours pour une faute du deuxième degré et quinze jours pour une faute du troisième degré ;

3. Considérant que doit être regardé comme dangereux, au sens de l'article D. 249-1 du Code de procédure pénale dont les dispositions sont désormais reprises à l'article R. 57-7-1 de ce code, tout objet dont on peut raisonnablement craindre, en raison notamment de la facilité de son usage, que l'utilisation en soit susceptible de mettre en cause la sécurité des personnes et des biens, notamment dans l'enceinte pénitentiaire ; que la possession d'un téléphone portable par un détenu, compte tenu de l'usage qui peut en être fait, notamment pour s'affranchir des règles particulières applicables, en vertu de l'article 727-1 du Code procédure pénale, aux communications téléphoniques des détenus et pour faire échec aux mesures de sécurité prises dans l'établissement pénitentiaire, doit être regardée comme la détention d'un objet dangereux et constitue ainsi une faute disciplinaire du premier degré ; qu'en jugeant le contraire, la cour administrative d'appel de Nancy a donné aux faits de l'espèce une qualification juridique erronée ;

4. Considérant qu'il résulte de ce qui précède que, sans qu'il soit besoin d'examiner l'autre moyen du pourvoi, le ministre de la Justice est fondé à demander l'annulation de l'arrêt attaqué en tant qu'il a annulé la décision du 22 mai 2008 du directeur interrégional des services pénitentiaires de Strasbourg ;

5. Considérant qu'il y a lieu, dans les circonstances de l'espèce, de régler l'affaire au fond dans la limite de la cassation prononcée, en application des dispositions de l'article L. 821-2 du Code de justice administrative ;

6. Considérant, d'une part, que M. B... n'apporte aucun élément à l'appui de ses allégations selon lesquelles certaines pièces n'auraient pas figuré dans le dossier auquel il a eu accès pour préparer sa défense devant la commission de discipline ;

7. Considérant, d'autre part, qu'il ressort des pièces du dossier et qu'il n'est pas sérieusement contesté par M. B... qu'un téléphone

portable en fonctionnement, dont il a fait usage à plusieurs reprises pour communiquer avec des personnes extérieures, a été découvert à ses côtés dans la salle de sports de la maison centrale d'Ensisheim ; que le moyen tiré de ce que le directeur interrégional des services pénitentiaires de Strasbourg se serait fondé sur des faits matériellement inexacts ne peut, par suite, qu'être écarté ;

8. Considérant qu'il résulte de ce qui précède que M. B…n'est pas fondé à demander l'annulation de la décision du 22 mai 2008 du directeur interrégional des services pénitentiaires de Strasbourg ;

DÉCIDE :

Article 1er : Les articles 2 et 3 de l'arrêt du 23 septembre 2010 de la cour administrative d'appel de Nancy sont annulés.

Article 2 : Les conclusions de la demande de M. B…tendant à l'annulation de la décision du 22 mai 2008 du directeur interrégional des services pénitentiaires de Strasbourg sont rejetées.

Article 3 : La présente décision sera notifiée à la garde des Sceaux, ministre de la Justice et à M. À… B....

[……]

Arrêt du 14 mai 2013 de la Chambre criminelle de la Cour de cassation nº 11-86626

LA COUR DE CASSATION, CHAMBRE CRIMINELLE, a rendu l'arrêt suivant :

Statuant sur le pourvoi formé par :

– Mme Martine X…, partie civile,

contre l'arrêt de la chambre de l'instruction de la cour d'appel de Bordeaux, en date du 9 août 2011, qui, dans l'information suivie contre personne non dénommée du chef de violation du secret de l'instruction, a prononcé l'annulation d'actes de la procédure et confirmé l'ordonnance de non-lieu rendue par le juge d'instruction ;

[……]

Sur le moyen unique de cassation, pris de la violation des articles 6 et 10 de la Convention européenne des droits de l'homme, 112-4 du Code pénal, 56-2, 60-1, 99-3, 593 du Code de procédure pénale, défaut de motifs, manque de base légale ;

« En ce que l'arrêt attaqué a ordonné l'annulation des cotes E 9, E 10, E 11 à E 14 (réquisitions adressées par les policiers aux opérateurs de téléphonie) et la cancellation subséquente de certains passages aux cotes E 5 et E 18 ;

« Aux motifs que, par commission rogatoire du 12 novembre 2009, en exécution de l'arrêt de la chambre de céans du 22 octobre précédent ordonnant un supplément d'information, le juge d'instruction délégué a saisi l'Inspection générale de la Police nationale aux fins de requérir les différents opérateurs téléphoniques aux fins de déterminer de quelles lignes téléphoniques étaient titulaires MM. Y... et A..., journalistes du quotidien *Sud-Ouest*, entre les 20 janvier et 5 février 2007, d'obtenir les facturations détaillées correspondant à ces numéros et de retranscrire les CD-Roms des factures détaillées obtenues dans le cadre des commissions rogatoires précédentes ; que figurent au dossier de la procédure (cote E 9, annexe 8, et E 10, annexe 1 à 6) les procès-verbaux des 6 août 2010 et 11 août 2011 auxquels sont jointes les retranscriptions des appels émis et reçus par les journalistes pour la période du 22 janvier au 5 février 2007 ainsi que les diverses réquisitions adressées par les policiers aux opérateurs de téléphonie afin d'obtenir la facturation détaillée de lignes attribuées à ces journalistes (E 11 à E 14) ; que la loi du 4 janvier 2010 a tendu à renforcer la protection des sources des journalistes ; que l'article 2 de la loi du 29 juillet 1881 énonce à présent : " il ne peut être porté atteinte directement ou indirectement au secret des sources que si un impératif prépondérant d'intérêt public le justifie et si les mesures envisagées sont strictement nécessaires et proportionnées au but légitime poursuivi" ; qu'il sera rappelé que la Cour européenne des droits de l'homme, depuis longtemps et de manière constante, en soulignant que la liberté d'expression représente l'un des fondements essentiels d'une société démocratique et que les garanties accordées à la presse revêtent une importance particulière, considère que la protection des sources journalistiques constitue l'une des pierres angulaires de la liberté de la presse et que toute ingérence, toute atteinte ou toute limitation apportée à la confidentialité des sources des journalistes ne saurait se concilier avec l'article 10 de la CEDH, d'où résulte le droit pour un journaliste de ne pas révéler ses sources, que si elle se justifie par un impératif prépondérant d'intérêt public et qu'elle est nécessaire, que la restriction est proportionnelle au but légitime poursuivi (CEDH, 27 mars 1996, *B...c. Royaume-Uni*, nº 39 et s. ; 25 février 2003, *C... et D... c. Luxembourg*, nº 46 à 60 ; 15 juillet 2003, *F...c. Belgique* ; 27 février 2008 *G...c. Belgique*, nº 53 à 68, *Sonoma Z... c. Pays-Bas*, 14 septembre 2010 nº 90 à 100) ; qu'ainsi que le rappelle également la Cour européenne, le droit des journalistes à taire leurs sources ne saurait être considéré comme un simple privilège qui leur serait accordé en fonction de la licéité ou de l'illicéité des sources mais représente un véritable attribut du droit à l'information, à traiter avec la plus grande circonspection (*G... c/ Belgique* précité nº 65) ; qu'elle ajoute que l'autorité publique doit démontrer que la balance des intérêts en présence, à savoir, d'une part, la protection des sources, pierre angulaire de la liberté de la presse dans une société démocratique, d'autre part, la prévention et la répression d'infractions, a été préservée (décisions précitées) ; que la méthode d'analyse dont a usé la CEDH dans ses décisions précitées (B..., § 45, C... § 58 précités), a consisté à déterminer avec une particulière circonspection si, *in concreto*,

"la balance des intérêts en présence, à savoir, d'une part, la protection des sources et de l'autre, la prévention et la répression d'infractions, a été préservée", cette juridiction ajoutant que "les considérations dont les institutions de la Convention doivent tenir compte font pencher la balance des intérêts en présence en faveur de la défense de la liberté de la presse dans une société démocratique ; que le législateur, s'inspirant des principes énoncés par la Cour européenne, a entendu protéger les sources des journalistes des atteintes tant directes qu'indirectes, comme celles consistant pour un magistrat à rechercher l'origine des informations détenues par un journaliste en recourant à des réquisitions pour obtenir ses relevés téléphoniques mettant en évidence les personnes avec lesquelles il a été en contact et qui ont constitué de possibles sources ; que les travaux parlementaires ont abordé expressément l'utilisation de ce procédé qui ne peut être légitimement motivée que par un impératif prépondérant d'intérêt public et justifiée par la nécessité d'une telle mesure, ces deux conditions étant cumulatives ; que le législateur a entendu également faire figurer dans l'article 2 précitée *in fine*, l'interprétation qu'il entendait donner à ces exigences en précisant, qu'au cours d'une procédure pénale, il devait être tenu compte, pour apprécier la nécessité de l'atteinte portée à la protection des sources, de la gravité du crime ou du délit, de l'importance de l'information recherchée pour la répression ou la prévention de cette infraction et du fait que les mesures d'investigations envisagées sont indispensables à la manifestation de la vérité ; qu'en outre, il a complété l'article 60-1 du Code de procédure pénale d'une disposition sanctionnant par la nullité le versement au dossier des éléments obtenus par une réquisition qui serait prise en violation de l'article 2 de la loi sur la liberté de la presse ; qu'en l'espèce, l'instruction a été ouverte par le procureur de la République du chef de violation du secret de l'instruction à la suite de la plainte déposée par Mme X..., laquelle déduisait de l'examen comparatif de la chronologie de son placement en garde à vue et de celle des articles parus dans le journal *Sud-Ouest* que les informations publiées par les journalistes sur l'objet et le déroulement de l'enquête ne pouvaient provenir que de policiers ou de magistrats ; que les réquisitions, qui avaient pour objet de porter indirectement mais nécessairement une atteinte au droit éminent des journalistes concernés à ne pas révéler leurs sources, ont donc été délivrées dans le cadre d'une information ouverte à partir des seules conjectures d'une plainte invoquant des « fuites » d'informations relatives à un placement en garde à vue et au déroulement de l'enquête ; qu'à supposer que la répression d'une infraction pénale soit toujours considérée comme un but légitime, il convient de souligner qu'en l'espèce, les actes ont porté sur la dénonciation par un particulier de la simple probabilité de la commission d'un délit de violation du secret de l'instruction, déduite de la succession à délai très rapproché d'un placement en garde à vue et d'informations parues dans la presse ; que, dans un tel contexte, la première condition à la légalité d'une atteinte portée au secret des sources, telle que l'a fixée restrictivement le législateur, à savoir l'existence d'un impératif prépondérant d'intérêt public qui la

justifie, n'a pas été remplie ; qu'il sera surabondamment fait observer que, pour apprécier la proportionnalité des mesures envisagées au but légitime poursuivi, le législateur a également précisé qu'il devait être tenu compte, non seulement de la gravité du crime ou du délit, de l'importance de l'information recherchée pour la prévention ou répression de cette infraction mais encore du fait que les mesures d'investigations envisagées sont indispensables à la manifestation de la vérité ; qu'en l'espèce, l'atteinte portée au droit fondamental à la protection des sources des journalistes, pierre angulaire de la liberté de la presse dans une société démocratique, apparaît en tout état de cause disproportionnée, dès lors qu'elle a été commise à partir de simples suppositions des parties civiles sur une violation du secret de l'instruction échafaudées sur la base des seuls éléments ci-dessus rapportés ; qu'elle ne répond pas à l'exigence de proportionnalité posée tant par la Cour européenne des droits de l'homme que par le législateur interne ; qu'en conséquence, les réquisitions visant à des investigations sur les téléphones des journalistes précités, qui ont été prises sans leur accord, en violation manifeste tant de l'article 10 de la CEDH que de l'article 2 de la loi du 29 juillet 1881, doivent être annulées ; que l'annulation prononcée s'étendra à tous les éléments dont elles sont le support nécessaire ;

« 1) alors que l'application immédiate de la loi nouvelle est sans effet sur la validité des actes accomplis conformément à la loi ancienne ; que l'article 2 de la loi du 29 juillet 1881, et les dispositions selon lesquelles "à peine de nullité, ne peuvent être versés au dossier les éléments obtenus par une réquisition prise en violation de l'article 2 de la loi du 29 juillet 1881 sur la liberté de la presse", sont issues de la loi nº 2010-1 du 4 janvier 2010 ; qu'en annulant les réquisitions adressées aux opérateurs de téléphonies, effectuées en exécution de commissions rogatoires des 29 mars 2007, 23 janvier 2008 et 12 novembre 2009, et les retranscriptions subséquentes, aux motifs que ces réquisitions avaient été prises en violation de l'article 2 de la loi du 29 juillet 1881 issu de la loi du 4 janvier 2010, et sans l'accord des journalistes, la chambre de l'instruction a violé l'article 112-4 du Code de procédure pénale ;

« 2) alors que s'agissant de réquisitions adressées non aux journalistes eux-mêmes, mais à des tiers non visés par les articles 56-1 à 56-3, l'accord de ces journalistes n'était pas requis ; qu'en se fondant sur le fait que les réquisitions adressées aux opérateurs de téléphonie avaient été prises sans l'accord des journalistes pour les annuler, la chambre de l'instruction a violé les articles 99-3, 60-1, alinéa 2, et 56-2 du Code de procédure pénale ;

« 3) alors que la contradiction de motifs équivaut à une absence de motifs, que l'arrêt ne peut, sans se contredire, retenir que les réquisitions avaient été délivrées à partir de simples conjectures ou suppositions d'une violation du secret de l'instruction de la part de la partie civile tout en constatant qu'entre le début de la garde à vue le 22 janvier 2007 à 10 heures 05, et la fin de la garde à vue le 24 janvier à 10 heures,

c'est-à-dire en un temps qui était celui exclusivement visé par la plainte- où la procédure était confinée entre les mains des services de la police et des magistrats, le journal *Sud-Ouest* avait publié des éléments précis de l'enquête tels que la description du cadre de l'enquête, de la plainte initiale, de son auteur, le nom des personnes gardées à vue, l'évocation de la prolongation de la mesure de garde à vue et la mention de la longueur des auditions, puis, dans son édition du 25 janvier, de nouveaux éléments très précis (contenu d'écoutes téléphoniques, résultat des perquisitions, aveux de certains mis en causes, annonce du contenu des réquisitions tendant à la mise en examen et au placement en détention provisoire) ;

« 4) alors que toute plainte est par essence conjecturale et doit être vérifiée par des mesures d'enquête ; qu'en l'espèce, la partie civile avait pris soin de circonscrire l'objet de sa plainte à la publication, dans plusieurs éditions, d'éléments précis de l'enquête en un temps où la procédure était confinée entre les mains des services de la police et des magistrats, de sorte qu'il ne s'agissait plus que d'identifier l'auteur de la fuite ; qu'en statuant par des motifs qui subordonnent en définitive l'existence d'un impératif prépondérant d'intérêt public justifiant la délivrance des réquisitions litigieuses à la démonstration préalable, par la partie civile, de l'identité de l'auteur des faits dénoncés, la chambre de l'instruction a statué par un motif inopérant ;

« 5) alors que sont justifiées par un impératif prépondérant d'intérêt public tiré de la répression et de la prévention des infractions, de la protection de la présomption d'innocence et de l'impartialité du pouvoir judiciaire, et sont strictement nécessaires et proportionnées au but légitime poursuivi, les réquisitions, limitées dans le temps, adressées à des opérateurs de téléphonie, à l'effet d'identifier les sources de journalistes, dès lors qu'elles ont été autorisées par un juge d'instruction, dans le cadre d'une plainte pour violation du secret de l'instruction dénonçant la divulgation par voie de presse, au fur et à mesure de sa progression, d'éléments précis de l'enquête en un temps parfaitement circonscrit celui de la garde à vue - où la procédure était confinée entre les mains des services de la police sous le contrôle d'un juge d'instruction, et alors que les journalistes entendus s'étaient retranchés derrière le secret des sources, et que les auditions des policiers comme l'exploitation de la facture détaillée du standard téléphonique du commissariat n'avaient rien donné, de sorte que l'identification des auteurs de l'infraction passait nécessairement par cette mesure d'investigation ; qu'en décidant le contraire, la chambre de l'instruction a méconnu les articles 6 et 10 de la Convention européenne des droits de l'homme, ensemble, à les supposer applicables, les dispositions de l'article 2 nouveau de la loi sur la liberté de la presse issues de la loi du 4 janvier 2010 » ;

Vu l'article 593 du Code de procédure pénale ;

Attendu que tout arrêt de la chambre de l'instruction doit comporter les motifs propres à justifier la décision et répondre aux articulations essentielles des mémoires des parties ; que l'insuffisance ou la contradiction des motifs équivaut à leur absence ;

Attendu qu'il résulte de l'arrêt attaqué et des pièces de la procédure que, le 22 janvier 2007, les services de police, agissant sur commission rogatoire d'un juge d'instruction saisi de faits de vol contre personne non dénommée, ont procédé, notamment, à des perquisitions au domicile et au cabinet de Mme X..., avocat ; que celle-ci a été placée en garde à vue le 22 janvier 2007 à 10 h 05, puis déférée devant le juge d'instruction, qui l'a mise en examen, le 25 janvier 2007 ;

Attendu que, le 23 janvier 2007 au matin, le journal *Sud-Ouest* a publié un article intitulé «Trois notables en garde à vue» dans lequel Mme X... était désignée ; que, dans son édition du lendemain, puis dans celle du 25 janvier 2007, de nouvelles précisions ont été apportées concernant, notamment, le déroulement de sa garde à vue ;

Attendu que Mme X... a porté plainte auprès du procureur de la République du chef de violation du secret de l'instruction, en soutenant que des révélations avaient été faites par la presse à un moment où la procédure n'était connue que du juge d'instruction et des officiers de police judiciaire agissant sur sa délégation, toutes personnes soumises à ce secret ; que, le 20 février 2007, ce magistrat a ouvert une information visant la plainte de Mme X..., qui s'est constituée partie civile ;

Attendu que le juge d'instruction saisi a procédé ou fait procéder à de nombreux actes tendant à l'identification des auteurs d'une éventuelle violation du secret de l'instruction ; que, notamment, par commission rogatoire du 23 janvier 2008, il a ordonné que soient produites les facturations détaillées des numéros de téléphone communiqués par plusieurs journalistes concernés ou tout autre numéro qui leur était attribué pour la période comprise entre le 20 janvier et le 5 février 2007 et demandé que soient identifiés les titulaires des numéros entrants ou sortants ; que ce magistrat a donné mission au délégataire de déterminer si les journalistes avaient été en contact avec les fonctionnaires de police mis en cause par la partie civile au moment de la commission des faits ; que des réquisitions à cette fin ont été adressées aux opérateurs téléphoniques et qu'un cédérom crypté a été versé au dossier, comprenant les facturations détaillées des abonnements de quatre journalistes, rédacteurs des articles en cause ;

Attendu que, le 24 avril 2009, le juge d'instruction a rendu une ordonnance de non-lieu, dont Mme X... a interjeté appel ; que, par arrêt du 22 octobre 2009, la chambre de l'instruction a ordonné un supplément d'information, tendant notamment à la communication de relevés de factures détaillées des journalistes concernés et à la transcription des

cédéroms déjà versés au dossier ; que les juges d'instruction commis ont délivré une commission rogatoire à cette fin, exécutée au mois d'août 2010, et ont procédé à différentes auditions avant de faire retour de la procédure à la chambre de l'instruction ;

Attendu que cette juridiction, après avoir prononcé l'annulation d'actes de la procédure effectués en exécution du supplément d'information, a confirmé l'ordonnance de non-lieu ;

Attendu que, pour annuler les réquisitions tendant à l'exécution d'investigations destinées à déterminer les lignes téléphoniques attribuées à des journalistes et les facturations détaillées correspondant à ces lignes, ainsi que les actes en étant le support nécessaire, l'arrêt retient que ces réquisitions ont été prises, sans l'accord des journalistes, en violation de l'article 10 de la CEDH et de l'article 2 de la loi du 29 juillet 1881, dans sa rédaction issue de la loi du 4 janvier 2010 ; que les juges ajoutent que lesdites réquisitions, qui avaient pour objet de porter atteinte au droit des journalistes concernés de ne pas révéler leurs sources, ont eu pour origine la dénonciation, par un particulier, de la simple probabilité de la commission d'un délit de violation du secret de l'instruction déduite de la succession à délai très rapproché d'un placement en garde à vue et d'informations parues dans la presse ; qu'ils en concluent qu'en l'espèce, l'existence d'un impératif prépondérant d'intérêt public n'était pas avérée et que l'atteinte portée au secret des sources, à partir de simples suppositions des parties civiles, était disproportionnée ;

Mais attendu qu'en se déterminant par ces seuls motifs, d'une part, sans mieux s'expliquer sur l'absence d'un impératif prépondérant d'intérêt public alors que la violation du secret de l'instruction reprochée imposait de rechercher les auteurs de cette infraction ayant porté atteinte à la présomption d'innocence, d'autre part, sans caractériser plus précisément le défaut de nécessité et de proportionnalité des mesures portant atteinte au secret des sources des journalistes au regard du but légitime poursuivi, et enfin, en faisant à tort référence à l'obligation d'obtenir l'accord des journalistes pour procéder aux réquisitions litigieuses alors qu'un tel accord n'est nécessaire que si ces professionnels sont directement requis de fournir des informations, la chambre de l'instruction n'a pas justifié sa décision ;

D'où il suit que la cassation est encourue ;

Par ces motifs :

CASSE et ANNULE, en toutes ses dispositions, l'arrêt susvisé de la chambre de l'instruction de la cour d'appel de Bordeaux, en date du 9 août 2011, et pour qu'il soit à nouveau jugé, conformément à la loi.

Arrêt du 22 octobre 2013 de la Chambre criminelle de la Cour de cassation no 13-81.945

LA COUR DE CASSATION, CHAMBRE CRIMINELLE, a rendu l'arrêt suivant :

Statuant sur le pourvoi formé par :

– M. Mohamed X...,

contre l'arrêt de la chambre de l'instruction de la cour d'appel de PARIS, 1re section, en date du 28 février 2013, qui, dans l'information suivie contre lui des chefs notamment, d'association de malfaiteurs en vue de la préparation d'actes de terrorisme, a prononcé sur sa demande d'annulation d'actes de la procédure ;

Vu l'ordonnance du président de la chambre criminelle, en date du 26 avril 2013, prescrivant l'examen immédiat du pourvoi ;

Vu le mémoire produit ;

[……]

[...] Mais sur le premier moyen de cassation, pris de la violation des articles 6 et 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, 12, 14, 41, 77-1-1 du Code de procédure pénale, 593 du même code, défaut de motifs, manque de base légale ;

« en ce que l'arrêt attaqué a dit n'y avoir lieu à annulation d'un acte ou d'une pièce de la procédure examinée jusqu'à la cote D 3304, rejetant ainsi la demande de nullité des mesures prévoyant la géolocalisation de M. X et des actes subséquents dans le cadre de l'enquête préliminaire ;

« aux motifs que la technique d'enquête de géo-localisation par suivi du téléphone mobile afin de surveiller les déplacements d'un individu ne fait l'objet d'aucun texte spécifique en l'état du droit français ; qu'il convient en conséquence d'analyser ce dispositif au regard des textes de procédure pénale en vigueur à ce jour ; que les articles 12, 14 et 41 du Code de procédure pénale confient à la police judiciaire le soin de "constater les infractions à la loi pénale, d'en rassembler les preuves et d'en rechercher les auteurs" sous le contrôle du procureur de la République; que les techniques de filatures et de surveillances effectuées par les policiers dans le cadre de leurs enquêtes trouvent leur fondement dans ces dispositions ; que les opérations querellées, dont la possibilité technique est par ailleurs notoirement connue des citoyens, donc prévisible, sans interception du contenu des conversations téléphoniques, sont de simples actes d'investigations techniques qui ne portent pas atteinte à la vie privée et au secret de correspondances ; qu'il existe aucun élément de contrainte ou de coercition, ni d'intrusion dans un véhicule ou dans un quelconque lieu privé ; que les investigations effectuées selon

ce procédé sont moins susceptibles de porter atteinte aux droits d'une personne que des méthodes de surveillance par des moyens visuels ou acoustiques qui révèlent plus d'informations sur la conduite, les opinions ou les sentiments de la personne qui en fait l'objet ; que la base légale de la géolocalisation n'est donc pas contestable ; que l'exigence normative est donc remplie et qu'il est légitime qu'elle fasse l'objet d'une interprétation judiciaire ; que ces actes, qui n'entrent pas dans le champ d'application de l'article 5 § 3 de la Convention européenne des droits de l'homme relatif au contrôle de la privation de liberté et relèvent donc bien de la compétence et des pouvoirs attribués au ministère public, ne sont pas contraires à l'article 8 de la Convention européenne, lequel prévoit des restrictions posées au principe par cet article, notamment pour la prévention des infractions ; qui s'agissant néanmoins de surveillances secrètes par les autorités publiques, il convient donc de vérifier les circonstances de la cause, en particulier au regard de la nature, de l'étendue et la durée des mesures et des raisons de leur mise en place ; qu'en l'espèce, l'enquête préliminaire avait été ouverte par la section antiterroriste du Parquet de Paris courant octobre 2011 suite à des informations parvenues à la DCRI selon lesquelles M. X, fondateur du site « ...Y... », aurait fédéré un certain nombre de personnes qui suivraient des entraînements physiques et un endoctrinement religieux pour se préparer au *jihad* ; qu'outre le caractère de propagande projihadiste de ce site, M. X avait tenu à plusieurs reprises des propos légitimant la riposte armée, le droit à la légitime défense en réaction à l'islamophobie en France et qu'il était en relation avec plusieurs personnes connues pour leurs liens avec la mouvance terroriste internationale ; que l'utilisation de la technique de géo-localisation par le biais du téléphone portable a donc été justifiée par la nécessité de vérifier l'existence d'une éventuelle préparation d'actes criminels, en particulier des faits d'attentats terroristes sur le territoire national, de détentions d'armes ou de produits explosifs, d'en rechercher l'organisation, d'en identifier les participants et de prévenir leur commission et ce, de manière discrète et efficace, en raison du caractère clandestin de ce type de délinquance ; que les infractions de cette nature troublent de façon évidente l'ordre public par leurs conséquences notamment humaines, à travers l'utilisation d'armes et la détermination de leurs auteurs dont la dangerosité concerne non seulement les victimes directes de leurs méfaits mais aussi les personnes se trouvant à proximité, ainsi que les services de police intervenant pour faire cesser les infractions ou procéder à l'arrestation des auteurs ; qu'en conséquence, la mesure de géolocalisation a répondu à une finalité légitime proportionnée à la gravité des infractions commises ou suspectées au regard de l'ordre public, strictement limitée aux nécessités de la manifestation de la vérité ; que contrairement à ce qui est soutenu par le conseil du requérant, la durée de la mesure a été précisément fixée dans les réquisitions, à savoir une durée de dix jours ; que les policiers ont donc agi dans l'exercice de leur mission ci-dessus rappelée et qu'il doit en conséquence être constaté que les réquisitions contestées n'ont méconnu ni les dispositions légales, ni les dispositions conventionnelles invoquées ;

"1°) alors qu'une mesure dite de « géolocalisation » consistant à surveiller les déplacements d'une personne par le suivi de son téléphone mobile constitue une ingérence dans la vie privée de cette personne, qui ne peut être légalement effectuée que dans les conditions prévues par l'article 8, alinéa 2, de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ; que l'ingérence doit donc être prévue par une loi présentant les qualités requises par la jurisprudence de la Cour européenne dans son interprétation de l'article 8, alinéa 2, indépendamment du caractère proportionné ou nécessaire de la mesure qui est par ailleurs et cumulativement requis ; qu'il est constant qu'aucune loi ne prévoit ni n'organise la surveillance des téléphones portables et de leurs déplacements, la « connaissance notoire » supposée des citoyens à cet égard ne pouvant pallier l'absence de loi suffisamment précise, accessible, prévisible et émanant d'un organe compétent pour la créer ; que ne répondent pas à ces exigence les textes très généraux des articles 12, 14 et 41 du Code de procédure pénale, relatifs à la mission de la police judiciaire ; que la chambre de l'instruction a violé l'article 8, alinéa 2, de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, et les textes susvisés ;

"2°) alors qu'une loi, au sens de l'article 8, alinéa 2, de la Convention, ne peut organiser une ingérence dans la vie privée des personnes qu'à la condition d'en placer la surveillance et l'exécution sous le contrôle de l'autorité judiciaire, ce n'est pas le Parquet, qui n'est pas indépendant et qui poursuit l'action publique ; que la chambre de l'instruction a encore violé les textes précités ;

"3°) alors qu'une loi ne répond aux qualités requises par l'article 8 alinéa 2 de la Convention pour justifier une ingérence dans la vie privée qu'à condition de prévoir des limites, notamment dans le temps, aux mesures de surveillance et d'en organiser la fin ou l'extinction ; que la chambre de l'instruction a, en validant les géolocalisations contestées, violé les textes susvisés" ;

Vu l'article 8 de la Convention européenne des droits de l'homme ;

Attendu qu'il se déduit de ce texte que la technique dite de « géolocalisation » constitue une ingérence dans la vie privée dont la gravité nécessaire qu'elle soit exécutée sous le contrôle d'un juge ;

Attendu que, pour écarter le moyen de nullité pris du défaut de fondement légal de la mise ne place, par les opérateurs de téléphonie, d'un dispositif technique, dit de « géolocalisation », permettant, à partir du suivi des téléphones de M. X de surveiller ses déplacements en temps réel, au cours de l'enquête préliminaire, l'arrêt retient, notamment, les articles 12, 14 et 41 du Code de procédure pénale, d'en rassembler les preuves et d'en rechercher les auteurs, sous le contrôle du procureur de la République, que les juges ajoutent que les mesures critiquées trouvent leur fondement dans ces textes, et qu'il s'agit de simples investigations techniques ne portant pas atteinte à la vie privée et n'impliquant pas

de recourir, pour leur mise en œuvre, à un élément de contrainte ou de coercition ;

Mais attendu qu'en se déterminant ainsi, la chambre de l'instruction a méconnu le texte conventionnel susvisé ;

D'où il suit que la cassation est encourue de ce chef ;

Par ces motifs :

CASSE et ANNULE, en ses seules dispositions relatives à la mesure de surveillance technique, dite de « géolocalisation », pratiquée au cours de l'enquête préliminaire, l'arrêt susvisé de la chambre de l'instruction de la cour d'appel de Paris, en date du 28 février 2013, toutes autres dispositions étant expressément maintenues ;

Et pour qu'il soit à nouveau jugé, conformément à la loi, dans les limites de la cassation ainsi prononcée,

Voir également, dans le même sens : arrêt du 22 octobre 2013 de la chambre criminelle de la Cour de cassation n°13-81.949.

Actualités parlementaires : l'examen du projet de loi relatif à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale

A la date d'achèvement de ce rapport, 30 octobre 2013, il est nécessaire de faire un point d'étape sur l'avancement des travaux parlementaires portant sur le projet de loi relatif à la programmation militaire pour les années 2014 à 2019, qui doit être promulgué d'ici la fin de l'année 2013.

Les développements qui suivent sont rédigés avec les précautions d'usage s'agissant d'un texte en cours de discussion par les assemblées parlementaires.

Le projet a été adopté en première lecture par la Haute-Assemblée le 21 octobre 2013 après plusieurs modifications par voie d'amendements parlementaires, en particulier dans les domaines portant sur le cadre légal du renseignement.

Ainsi, les sénateurs ont décidé d'étendre les prérogatives de la délégation parlementaire au renseignement au-delà de ce qu'envisageait le gouvernement initialement[1].

1) Voir chapitre 2 de la 1ère partie du présent rapport

De même, s'agissant de l'article 13 du projet de loi, destiné à donner une base légale précise à l'accès administratif à la géolocalisation en temps réel, les sénateurs ont adopté un amendement du Président de la Commission des lois, Jean-Pierre SUEUR, qui vise à unifier dès le 1er janvier 2015 les dispositifs de recueil de données techniques de communications (issus de la loi du 10 juillet 1991 et de celle du 23 janvier 2006) en créant un nouveau régime « d'accès administratif aux données de connexion », au sein duquel une procédure d'autorisation des mesures de géolocalisation en temps réel est prévue:

Article 13 du texte adopté le 21 octobre 2013 par le Sénat et transmis à l'Assemblée nationale

Rédiger ainsi cet article :

I. – Le code de la sécurité intérieure est ainsi modifié :

1° L'intitulé du titre IV du livre II est ainsi rédigé : « Interceptions de sécurité et accès administratif aux données de connexion » ;

2° Le titre IV du livre II est complété par un chapitre VI ainsi rédigé :

Chapitre VI

Accès administratif aux données de connexion

Art. L. 246-1. – Pour les finalités énumérées à l'article L. 241-2, peut être autorisé le recueil, auprès des opérateurs de communications électroniques et personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des prestataires mentionnés aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, des informations ou documents traités ou conservés par leurs réseaux ou services de communication électronique, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communication électronique, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelant, la durée et la date des communications.

Art. L. 246-2. – I. Les informations ou documents mentionnés à l'article L. 246-1 sont sollicités par les agents individuellement désignés et dûment habilités des services relevant des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget, chargés des missions prévues à l'article L. 241-2.

II. – Les demandes des agents sont motivées et soumises à la décision d'une personnalité qualifiée placée auprès du Premier ministre. Cette personnalité est désignée pour une durée de trois ans

renouvelable par la Commission nationale de contrôle des interceptions de sécurité sur proposition du Premier ministre qui lui présente une liste d'au moins trois noms.

Des adjoints pouvant la suppléer sont désignés dans les mêmes conditions. La personnalité qualifiée établit un rapport d'activité annuel adressé à la Commission nationale de contrôle des interceptions de sécurité. Les décisions, accompagnées de leur motif, font l'objet d'un enregistrement et sont communiquées à la Commission nationale de contrôle des interceptions de sécurité.

Art. L. 246-3. – Pour les finalités énumérées à l'article L. 241-2, les données prévues à l'article L. 246-1 peuvent être recueillies sur sollicitation du réseau et transmises en temps réel par les opérateurs aux agents visés au I de l'article L. 246-2.

L'autorisation est accordée, sur demande écrite et motivée des ministres de la sécurité intérieure, de la défense, de l'économie et du budget ou des personnes que chacun d'eux aura spécialement désignées, par décision écrite du Premier ministre ou des personnes spécialement désignées par lui, pour une durée maximale de dix jours. Elle peut être renouvelée dans les mêmes conditions de forme et de durée. Elle est communiquée dans un délai de quarante-huit heures au président de la Commission nationale de contrôle des interceptions de sécurité.

Si celui-ci estime que la légalité de cette décision au regard des dispositions du présent titre n'est pas certaine, il réunit la commission, qui statue dans les sept jours suivant la réception par son président de la communication mentionnée au premier alinéa.

Au cas où la commission estime que le recueil d'une donnée de connexion a été autorisé en méconnaissance des dispositions du présent titre, elle adresse au Premier ministre une recommandation tendant à ce qu'il y soit mis fin.

Elle porte également cette recommandation à la connaissance du ministre ayant proposé le recueil de ces données et du ministre chargé des communications électroniques.

Art. L. 246-4. – La Commission nationale de contrôle des interceptions de sécurité dispose d'un accès permanent au dispositif de recueil de données techniques mis en œuvre en vertu du présent chapitre afin de procéder à des contrôles visant à s'assurer du respect des conditions fixées aux articles L. 246-1 à 246-3. En cas de manquement, elle adresse une recommandation au Premier ministre. Celui-ci fait connaître à la commission, dans un délai de quinze jours, les mesures prises pour remédier au manquement constaté.

Les modalités d'application du présent article sont fixées par décret en Conseil d'État après avis de la Commission nationale de l'informatique

et des libertés et de la Commission nationale des interceptions de sécurité, qui précise notamment la procédure de suivi des demandes et les conditions et durée de conservation des données transmises.

Art. L. 246-5. – Les surcoûts identifiables et spécifiques éventuellement exposés par les opérateurs et personnes mentionnées au premier alinéa pour répondre à ces demandes font l'objet d'une compensation financière. » ;

3° Les articles L. 222-2, L. 222-3 et L. 243-12 sont abrogés ;

4° À la première phrase du premier alinéa de l'article L. 243-7, les mots : « de l'article L. 243-8 et au ministre de l'intérieur en application de l'article L. 34-1-1 du code des postes et des communications électroniques et de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique » sont remplacés par la référence : « des articles L. 243-8, L. 246-3 et L. 246-4 » ;

5° À l'article L. 245-3, après les mots « en violation », sont insérés les mots : « des articles L. 246-1 à L. 246-3 et ».

II. – L'article L. 34-1-1 du code des postes et des communications électroniques est abrogé.

III. – Le II bis de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique est abrogé.

IV. – Le présent article entre en vigueur le 1er janvier 2015.

Sur le fond, ce nouveau régime de recueil de données techniques s'inspirerait à la fois du dispositif relatif aux interceptions de communications de la loi de 1991 et de celui, temporaire et expérimental, propre à la prévention du terrorisme, créé par la loi du 23 janvier 2006.

Il pourrait ainsi être utilisé pour les mêmes finalités que celles prévues par le code de la sécurité intérieure pour les interceptions de sécurité (recherche des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous).

Les autorisations seraient données par une personnalité qualifiée placée auprès du Premier ministre et la CNCIS effectuerait un contrôle *a posteriori*, en ayant un accès permanent au dispositif technique de recueil des données, ainsi que la possibilité de recourir à la recommandation adressée au Premier ministre, procédure instituée par la loi de 1991.

Ce texte conforterait donc pleinement les apports de la loi du 10 juillet 1991 et le rôle de la CNCIS comme autorité indépendante de contrôle. Il confirmerait l'institution originale de la « personnalité qualifiée »

placée désormais auprès du Premier ministre et continuant de relever de l'autorité administrative indépendante pour son activité de traitement et de contrôle des requêtes.

Plus attentatoire à la vie privée, la géolocalisation en temps réel serait possible dans des conditions plus strictes que les autres recueils de données techniques, sur demande écrite et motivée du ministre de la défense, du ministre de l'intérieur ou du ministre chargé des douanes, ou des personnes que chacun d'eux aura spécialement désignées, et sur décision du Premier ministre.

Chaque autorisation de géolocalisation aurait une durée de validité limitée de dix jours, inférieure à celle prévue pour les interceptions de sécurité (article L. 242-3 du code de la sécurité intérieure). Toute mesure serait soumise au contrôle a posteriori de la CNCIS.

La présente réforme entrerait en vigueur le 1er janvier 2015.

Le texte adopté par le Sénat va dans le sens des préconisations formulées depuis plusieurs années par la CNCIS[1] et reprises lors des travaux par le sénateur Jean-Jacques HYEST, membre de la Commission, auteur d'un amendement en ce sens.

Néanmoins, comme l'a fait observer M. HYEST lors des débats du 21 octobre 2013, la CNCIS souhaite que dans le texte désormais transmis à l'Assemblée plusieurs points puissent être améliorés :

– La consécration par la loi de la pratique de l'avis préalable de la CNCIS pour les demandes de géolocalisation en temps réel comme pour les demandes d'interceptions de sécurité ;

– Un délai pour les autorisations de géolocalisation en temps réel qui soit plus bref que dix jours, la Commission recommandant de retenir la durée de 72 heures, renouvelable.

1) Voir section 5 chapitre 4 de la 1ère partie du présent rapport