

# Sommaire

<b>Avant-propos</b> .....	5
Première partie	
<b>RAPPORT D'ACTIVITÉ</b> .....	7
Chapitre I	
<b>Organisation et fonctionnement de la Commission</b> .....	9
Chapitre II	
<b>Le contrôle des autorisations</b> .....	13
Chapitre III	
<b>Le contrôle de l'exécution</b> .....	25
Chapitre IV	
<b>Le contrôle du matériel</b> .....	31
Chapitre V	
<b>Actualités de l'année 2006</b> .....	41

Deuxième partie

**ÉTUDES ET DOCUMENTS** ..... 43

Chapitre I

**Présentation ordonnée des textes relatifs aux interceptions**..... 45

Chapitre II

**Actualité législative** ..... 59

Chapitre III

**Observations sur les motifs légaux d'interception**..... 63

Chapitre IV

**Interceptions de sécurité et secret-défense** ..... 77

Chapitre V

**Jurisprudence européenne et française** ..... 79

Chapitre VI

**Questions parlementaires**..... 91

# Avant-propos

*Comme les années précédentes, notre rapport d'activité analyse de manière détaillée les statistiques dont nous disposons maintenant pour 2006. On constatera ainsi que le chiffre total des interceptions de sécurité accordées demeure inférieur à 6000, chiffre à rapprocher d'un parc téléphonique dépassant maintenant les 84 millions d'unités, lignes fixes et portables confondus.*

*Un commentaire détaillé est donné dans le corps même du rapport. Qu'il suffise de constater ici la hausse modérée (3,5%) de ce total et la réduction sensible des demandes présentées selon la procédure d'urgence absolue (17% contre 20,6% en 2005), réduction saluée par la Commission dans la mesure où l'examen hebdomadaire normal des demandes assure une meilleure qualité au contrôle.*

*Je souhaite rappeler dans cet avant-propos deux points de doctrine importants, et évoquer ensuite l'évolution du champ et des méthodes de contrôle de notre Commission.*

*Le premier point a trait à la qualité de la motivation des demandes. À cet égard un certain relâchement a pu être constaté dans le chef de quelques services. Ceci explique sans doute la hausse importante (plus 20%) des « demandes de renseignement complémentaires », méthode développée par la Commission pour sortir du système « binaire », trop réducteur, de l'avis défavorable opposé à l'avis favorable. Je voudrais rappeler ici avec une certaine solennité que le principe de la présomption d'innocence irrigue notre droit depuis 1789. La motivation doit donc faire état de présomptions sérieuses de la dangerosité de la cible, ou de la concrétisation d'une menace pesant par exemple sur notre sécurité nationale ou sur les éléments essentiels de notre patrimoine scientifique et économique.*

*Le second point concerne le caractère subsidiaire de l'écoute par rapport aux autres moyens de renseignement : observations de terrain et enquêtes d'environnement. Il existe en outre dans nos lois et règlements toute une panoplie de moyens de contrôle qui peuvent et doivent être mis en œuvre, avant que l'écoute ne vienne conforter si nécessaire les soupçons révélés par ceux-ci. Ceci doit permettre d'éviter que les interceptions de sécurité, soient « banalisées ». Pour ce même motif, l'interception de sécurité à caractère préventif, doit laisser place à l'interception judiciaire dès que suffisamment d'éléments sont réunis pour ouvrir une procédure.*

*La loi du 23 janvier 2006 relative à la lutte contre le terrorisme a confié une nouvelle responsabilité à la Commission. Elle a ajouté à cet effet un article 27 à la loi du 10 juillet 1991 et étendu la compétence de la Commission au contrôle des demandes de données techniques (identification d'un numéro, environnement « relationnel » de l'abonné, etc.) dont l'obtention apparaît nécessaire à la prévention des actes de terrorisme dans les conditions décrites au nouvel article 34-1-1 du Code des postes et des communications électroniques. Le décret d'application de la loi ayant été pris le 22 décembre 2006, la Commission a nommé le 26 décembre 2006, après avoir entendu les différents candidats, la « personnalité qualifiée » chargée aux termes de la loi d'approuver ou non les demandes dûment motivées. Elle devra en 2007 développer de nouvelles méthodes de contrôle dans ce champ d'activité qui demeure à explorer.*

*Pour ce qui est de son champ d'activité traditionnel défini par la loi de 1991, la Commission est confortée par les résultats de l'année 2006 dans sa conviction que la voie du dialogue loyal et constructif avec les services, et le développement pour certains dossiers sensibles du « contrôle continu » demeurent le gage du respect d'un équilibre, toujours délicat à maintenir, entre la protection des libertés et la sauvegarde des intérêts supérieurs de la Nation.*

Jean-Louis DEWOST  
*Président de la Commission*

Première partie

---

# RAPPORT D'ACTIVITÉ

# Organisation et fonctionnement de la Commission

## Composition de la Commission

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

- Jean-Louis DEWOST, président de section honoraire au Conseil d'État nommé président pour une durée de six ans par le président de la République (décret du 29 septembre 2003, publié au *Journal officiel* le 30 septembre 2003).
- Jacques BAUDOT, sénateur (UMP) de Meurthe-et-Moselle, désigné le 26 octobre 2004 par le président du Sénat.
- Bernard DEROSIER, député (PS) du Nord, désigné le 20 mars 2003 par le président de l'Assemblée nationale.

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

- Gérard LORHO, délégué général depuis sa nomination en date du 17 décembre 2001.
- Rémi RECIO, chargé de mission depuis le 19 décembre 2003.

Le secrétariat est assuré par Mesdames Nathalie BRUCKER et Françoise NUDELMANN.

Monsieur Franck DEMUYS conduit le véhicule de la Commission.

## Rappel des compositions successives de la Commission

### • *Présidents*

- Paul BOUCHET, conseiller d'État, 1<sup>er</sup> octobre 1991.
- Dieudonné MANDELKERN, président de section au Conseil d'État, 1<sup>er</sup> octobre 1997.
- Jean-Louis DEWOST, président de section au Conseil d'État, 1<sup>er</sup> octobre 2003.

### • *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.

### • *Représentants du Sénat*

- Marcel RUDLOFF, sénateur du Bas-Rhin, 17 juillet 1991.
- Jacques THYRAUD, sénateur du Loir-et-Cher, 26 mars 1992.
- Jacques GOLLINET, 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.

## Missions et Fonctionnement

La Commission est chargée de veiller au respect des dispositions du Titre II (« des interceptions de sécurité ») de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques.

Conformément à l'article 1<sup>er</sup> de son règlement intérieur, la Commission se réunit à l'initiative du président lorsque celui-ci estime que la légalité d'une autorisation d'interception n'est pas certaine.

Elle peut également être réunie à l'initiative de l'un de ses membres sur toute question relative à l'application du Titre II de la loi du 10 juillet 1991 relatif aux interceptions de sécurité.

Elle reçoit les réclamations des particuliers, procède en toute indépendance aux contrôles et enquêtes qui lui paraissent nécessaires à l'accomplissement de sa mission et s'attache à nouer tous contacts utiles à son information.

Conformément à l'article 16 de la loi, les ministres, autorités publiques et agents publics doivent prendre toutes mesures de nature à faciliter son action.

La Commission est également 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.

Elle est enfin représentée par ses agents aux réunions de la commission consultative créée par le décret n° 97-757 du 10 juillet 1997 qui, sous la présidence du secrétaire général de la défense nationale, émet des avis sur les demandes de commercialisation ou d'acquisition des matériels susceptibles de porter atteinte au secret des correspondances.

Le président remet avant publication le rapport annuel d'activité de la Commission au Premier ministre et aux présidents des deux Assemblées.

## Financement

Autorité administrative indépendante, la Commission nationale de contrôle des interceptions de sécurité dispose de crédits individualisés figurant au budget des services du Premier ministre. Le président est ordonnateur des dépenses (article 18 alinéa 2 de la loi).

Pour l'année 2006 et conformément à la déclinaison en programmes, actions et sous-actions de la loi organique relative aux lois de finances, le budget de la CNCIS a été inscrit au sein du programme 129 – Coordination du travail gouvernemental – action 08 – Défense et protection des libertés – où la Commission est regroupée avec la Commission consultative du secret de la défense nationale (CCSDN) et la Commission nationale de déontologie de la sécurité (CNDS).

Afin de respecter l'indépendance budgétaire de ces trois autorités indépendantes, chacune a été dotée d'un budget opérationnel de programme (BOP), celui de la CNCIS étant référencé 129AIC. Les crédits alloués se sont élevés à 544 204 euros dont 450 817 euros pour les dépenses du Titre II (dépenses de personnel) et à 93 387 euros pour les dépenses de fonctionnement.

Pour l'année 2007 les crédits du BOP CNCIS se décomposent en 489 265 euros pour le Titre II (dépenses de personnel) et 76 000 euros pour les autres titres (dépenses de fonctionnement) soit un total de 465 265 euros. L'augmentation des crédits de personnel est destinée à permettre à la Commission de faire face aux charges nouvelles de contrôle induites par l'article 6 de la loi n° 2006-64 du 23 janvier 2006 dont les effets sont attendus courant 2007.

Les crédits du BOP CNCIS sont destinés en priorité à permettre le fonctionnement continu et sécurisé de la CNCIS. La structure permanente de la Commission comprend à cet effet 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 estampillés secret-défense. La Commission doit disposer des moyens d'information les plus larges comme les plus spécialisés en source ouverte (presse et documentation). Elle doit également disposer d'un moyen propre pour assurer des déplacements discrets notamment pour effectuer des visites de contrôle. Elle est enfin tenue à la publication d'un rapport annuel. Les crédits de personnel et de fonctionnement alloués permettront, difficilement pour ce qui concerne le fonctionnement, de répondre à ces priorités.

---

# Le contrôle des autorisations

## Le contrôle en amont

### **Théorie et pratique**

La mission première de la CNCIS est la vérification de la légalité des autorisations d'interception. Elle se traduit par un contrôle systématique et exhaustif de l'ensemble des demandes.

La loi de 1991 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 14 de la loi du 10 juillet 1991. Ce contrôle *a priori* permet un dialogue utile avec les services demandeurs et une meilleure prise en compte par ceux-ci, dès le stade préparatoire, des éléments de la « jurisprudence » de la Commission grâce au relais centralisé que constitue le Groupement interministériel de contrôle (GIC).

Ce contrôle *a priori* a été étendu en 2003 aux interceptions demandées en urgence absolue en raison de leur part croissante et grâce à une disponibilité accrue de la Commission.

Enfin le président de la Commission est informé par le GIC des décisions prises par le Premier ministre ou les personnes déléguées par celui-ci dans les conditions prévues par la loi de 1991. En cas de désaccord, il soumet la divergence d'appréciation à la délibération de la Commission conformément à l'article 14 de la loi. Dans l'hypothèse où le désaccord est confirmé, une recommandation tendant à l'interruption

de l'interception en cause est adressée au Premier ministre. Il convient toutefois de noter que depuis la transmission pour avis *a priori* de l'intégralité des demandes d'interception cette disposition a perdu son intérêt sauf bien sûr pour ce qui concerne les interceptions déjà en cours et dont la Commission recommande l'interruption.

## Contrôle formel et respect des contingents

L'activité de contrôle 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 la multiplication des demandes urgentes et afin de fluidifier les procédures, la Commission a suggéré et obtenu que la loi n° 2006-64 du 23 janvier 2006 introduise à l'article 4 de la loi du 10 juillet 1991 une nouvelle disposition autorisant chaque ministre, à l'instar du Premier ministre, à déléguer de façon permanente sa signature à deux personnes.

Il convient de rappeler que 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. Ce système déjà mis en place par la décision du 28 mars 1960 du Premier ministre Michel Debré, mais résultant en tout état de cause à l'époque considérée de contraintes techniques (capacité maximale d'enregistrement sur des magnétophones à bandes ou à cassettes et capacité d'exploitation par le GIC) a été consacré en 1991 comme devant « inciter les services concernés à supprimer le plus rapidement possible les interceptions devenues inutiles, avant de pouvoir procéder à de nouvelles écoutes » (CNCIS 3<sup>e</sup> rapport 1994, p. 16).

Le système par lequel les interceptions sont contingentées – leur nombre doit à tout moment respecter un plafond fixé par ministère en vertu d'une décision du Premier ministre, la répartition interne entre services étant du ressort de chaque ministère – conduit à ce que **le nombre moyen annuel des interceptions est 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) à rapprocher du doublement du seul parc téléphonique au cours de la même période (1996-2006).

## Évolution des contingents d'interceptions prévus par l'article 5 de la loi du 10 juillet 1991

Tableau récapitulatif

Contingents	Initial 1991-1996	1997	2003	Juin 2005
Ministère de la Défense	232	330	400	450
Ministère de l'Intérieur	928	1 190	1 190	1 290
Ministère du Budget	20	20	80	100
<b>Total</b>	<b>1 180</b>	<b>1 540</b>	<b>1 670</b>	<b>1 840</b>

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

Le premier et le seul 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, directement inspirés du Livre IV du Code pénal qui incrimine les atteintes à ces intérêts fondamentaux, ne font que décliner les différents aspects de la sécurité, mais la référence précise à ceux-ci permet une première appréciation des demandes. Ces motifs, énumérés à l'article 3 de la loi, 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 la loi du 10 janvier 1936 sur les groupes de combat et les milices privées. Les services demandeurs doivent donc faire référence 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 et suffisamment consistante pour apprécier leur articulation et leur adéquation avec le motif légal.

À cet effet le cadre des imprimés de demandes a été revu courant 2006 pour tendre à partir des modèles les plus complets à une uniformisation de la présentation gage d'une meilleure égalité d'appréciation. La Commission attache du prix au caractère exhaustif des mentions notamment relatives aux interceptions précédentes ayant pu exister sur la même cible. Ces cadres ne doivent pas être perçus non plus comme un carcan dont on ne pourrait sortir, par exemple en présentant spontanément des informations complémentaires indispensables à l'appréciation de la demande.

Afin d'assurer un équilibre toujours délicat entre ces deux notions apparemment opposées, le contrôle 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 protéger plus particulièrement les 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 articulés et non pour une raison autre qui ne relèverait d'aucun motif légal, quelle que soit par ailleurs la véracité des faits rapportés.

La « jurisprudence » de la CNCIS s'attache également à la protection des libertés de conscience et d'expression. Ainsi maintient-elle que le prosélytisme religieux, comme l'expression d'opinions extrêmes, ne justifient pas en tant que tels une demande d'interception s'ils ne comportent aucune menace pour l'ordre public républicain, matérialisée par exemple par un appel ou un encouragement à la violence.

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 (*cf.* développements *infra* p. 63).

Le président de la CNCIS peut demander les éléments d'informations complémentaires qui lui sont nécessaires pour fonder son avis. Il formule également les observations qu'il juge utiles sur la pertinence du motif invoqué, procédant le cas échéant à des propositions de substitutions de motif. Il s'assure que la demande respecte le **principe de proportionnalité** entre le but recherché et la mesure sollicitée : la gravité du risque ou du danger pour la sécurité des personnes, qu'elles soient physiques ou 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 justifier cette atteinte. La recherche de cette proportionnalité peut se traduire *ab initio* ou lors du renouvellement (*cf. infra* p. 18) par une restriction au cas par cas de la durée de la mesure dont le maximum est de quatre mois, par l'instruction donnée d'exclure certaines parties strictement privées des conversations des transcriptions (appelées « productions ») et par des demandes de bilans circonstanciés avant aval d'une nouvelle prolongation dans le cas d'une interception déjà plusieurs fois renouvelée. Il faut enfin veiller à ce que soit respecté le **principe de subsidiarité** et, par conséquent, s'assurer que le but recherché ne puisse être aussi bien rempli par d'autres moyens (enquête de terrain, d'environnement, etc.).

## Le contrôle en aval

### Données chiffrées et commentaires

#### Évolutions 2005-2006

5985 interceptions de sécurité ont été réalisées en 2006 (4 176 interceptions initiales et 1 809 renouvellements), soit une **hausse modérée** de **3,5%** par rapport à 2005 (5774 dont 4067 interceptions initiales et 1707 renouvellements). Le caractère inchangé du contingent depuis juin 2005 explique cette quasi-stabilité. On relève toutefois une hausse plus sensible des renouvellements (6%) qui trouve en partie son explication dans un meilleur suivi de ceux-ci par un service par ailleurs gros demandeur, ce qui a nécessairement eu un impact statistique important.

S'agissant des interceptions initiales, 714 contre 854 en 2005 (soit une baisse de 15%) ont été présentées selon la procédure dite d'urgence absolue, soit 17% des demandes contre 20,6% en 2005. L'absence d'attentat majeur sur le territoire ou dans les pays limitrophes et l'abandon du recours abusif à l'urgence pour reconstruire des interceptions interrompues faute de renouvellements présentés dans les délais, expliquent cette forte baisse, compensée en partie par l'accord donné par la Commission au dernier trimestre à une extension des motifs de recours à l'urgence.

On rappellera que les urgences dites « techniques » étaient initialement destinées à pallier l'interruption de surveillance résultant d'un changement de numéro de la cible. Désormais, pour répondre au souci des services identifiant en cours d'interception un autre numéro utilisé concurremment par la même cible, sont également acceptées des interceptions en urgence de ce second numéro, toujours après examen préalable de la Commission.

Pour l'année 2006, 272 urgences techniques contre 214 en 2005 ont été présentées représentant 38% du total des urgences contre 25% l'année antérieure.

Pour ce qui concerne les motifs en dépit d'une menace terroriste de niveau élevé, c'est toujours la prévention de la criminalité et de la délinquance organisée qui reste le premier motif des demandes initiales avec 52,2% du total (contre 48,5% en 2005) suivie de la prévention du terrorisme avec 31,7% (contre 35,4% en 2005) et la sécurité nationale 14,7%. S'agissant des renouvellements on note que la prévention du terrorisme est en première place avec 43,8%, suivie de la sécurité nationale (40,6%) et de la prévention de la criminalité et délinquance organisées (13,6%). Au total, demandes initiales et renouvellements confondus, c'est la prévention de la criminalité organisée qui, cette année, se détache nettement avec 40,6% suivie de la prévention du terrorisme 35,2% et la sécurité nationale 22,6%, ces trois motifs représentant 98,5% des demandes.

## Observations

La Commission ayant poursuivi sa démarche de dialogue avec les services demandeurs afin d'aboutir à une logique d'avis moins binaire (avis favorable/avis défavorable), le nombre d'observations a encore crû passant de 613 en 2005 à 745 dont 148 demandes de renseignements complémentaires et 176 limitations de la durée d'observation sollicitée. Les avis défavorables, comptés dans les observations, sont en baisse (38 dont 25 sur demandes initiales dont 1 en urgence contre 102 en 2005). Une partie de cette baisse s'explique par une nette amélioration de la motivation par un service en particulier.

Par ailleurs les renseignements demandés ont conduit les services à ne pas donner suite à 6 demandes.

Force est également de constater que le contrôle en amont des demandes aussi minutieux et exhaustif soit il, ne saurait suffire. Le contrôle des « productions » (transcription des interceptions) est, en aval, le moyen privilégié pour s'assurer à la fois de la bonne adéquation de la demande au motif légal invoqué et de l'intérêt réel présenté par l'interception au regard des critères de proportionnalité et de subsidiarité. Ce « contrôle continu » s'effectue de manière aléatoire ou ciblée. Il permet ainsi à la Commission, en dépit de la charge matérielle qu'il génère, de prendre des décisions plus éclairées au stade du renouvellement de l'interception s'il est demandé par le service, et le cas échéant, de prendre en cours d'exploitation d'une interception, une recommandation tendant à l'interruption de cette dernière.

Ainsi, les « productions » (transcriptions) de 51 lignes interceptées en 2006 ont elles été examinées et la Commission a recommandé la cessation d'interception de 2 lignes. Elle n'a pas été suivie dans un cas par le Premier ministre. Par ailleurs, 3 lignes dont les productions étaient suivies depuis 2005 ont fait l'objet de recommandations de suppression toutes suivies par le Premier ministre. Trois autres lignes, dont les productions n'étaient pas suivies, ont également fait l'objet de recommandations de suppression également approuvées par le Premier ministre.

Finalement, lors de l'examen initial ou en cours d'interception, ce sont 46 avis défavorables à l'interception ou à la poursuite de celle-ci qui ont été émis tous suivis à l'exception d'un cas par le Premier ministre.

Au total avec 5985 interceptions accordées contre 5774 en 2005, on constate à nouveau que les interceptions de sécurité demeurent, au regard de vecteurs de communications électroniques en constante augmentation (près de 84 millions de portables et lignes fixes), la mesure d'exception voulue par la loi. Ce caractère exceptionnel est d'autant plus accusé que chaque vecteur intercepté compte pour une interception quel que soit le nombre de vecteurs utilisés par la cible. Dès lors, les 4 176 interceptions initiales concernent en réalité moins de 4000 personnes.

À titre de comparaison, on a dénombré environ 20500 interceptions judiciaires au cours de la même période.

## Tableaux annexes

### Les demandes initiales d'interception

#### État des demandes initiales d'interception, années 2005 et 2006

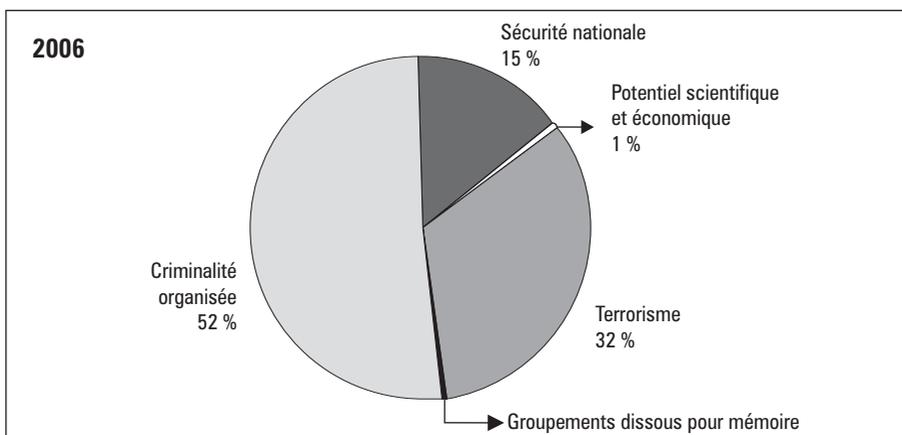
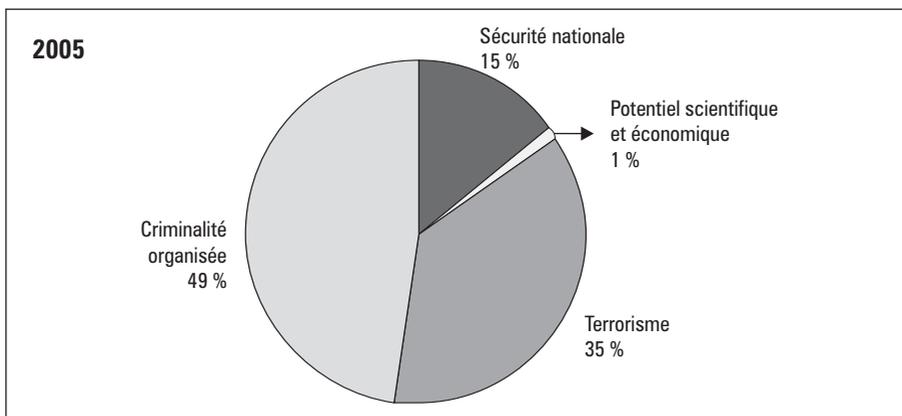
	Demandes initiales		Dont urgence absolue		Accordées	
	Année 2005	Année 2006	Année 2005	Année 2006	Année 2005	Année 2006
<b>Totaux</b>	4 144	4 203	854	714	4 067	4 176

#### État comparatif sur cinq ans

Motifs	2002	2003	2004	2005	2006
Sécurité nationale	486	526	548	625	622
Potentiel scientifique et économique	38	42	66	43	47
Terrorisme	1 103	1 126	1 292	1 468	1 330
Criminalité organisée	1 511	1 668	1 881	2 006	2 195
Groupements dissous	0	0	0	2	9
<b>Totaux</b>	<b>3 138</b>	<b>3 362</b>	<b>3 787</b>	<b>4 144</b>	<b>4 203</b>

## Demandes initiales

### Répartition des motifs

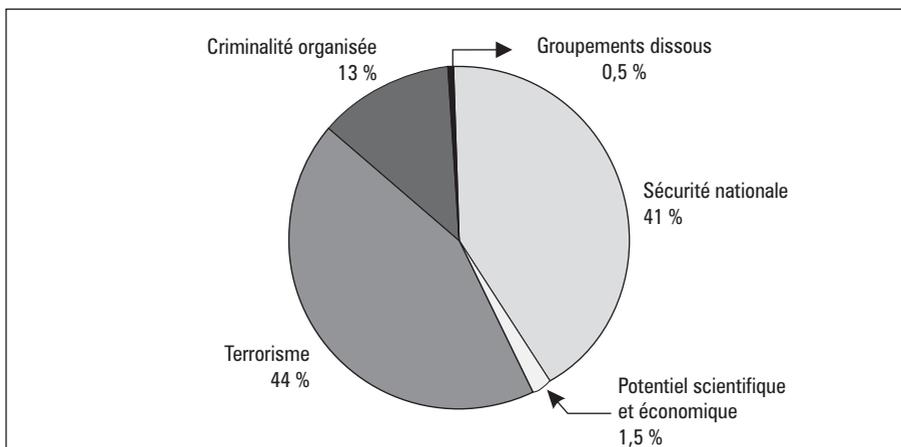


## Les renouvellements d'interception

Répartition des motifs (renouvellements accordés), année 2006

Sécurité nationale	Potentiel scientifique et économique	Terrorisme	Criminalité organisée	Groupements dissous	Total
735	28	794	243	9	1 809

## Les renouvellements d'interception



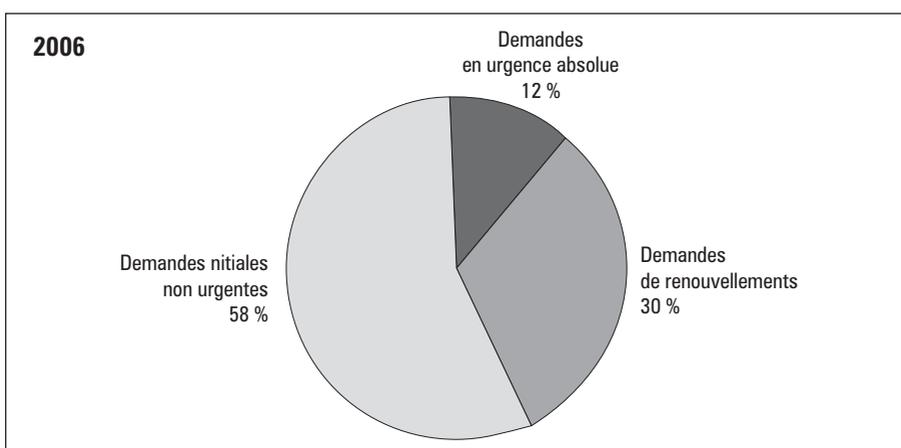
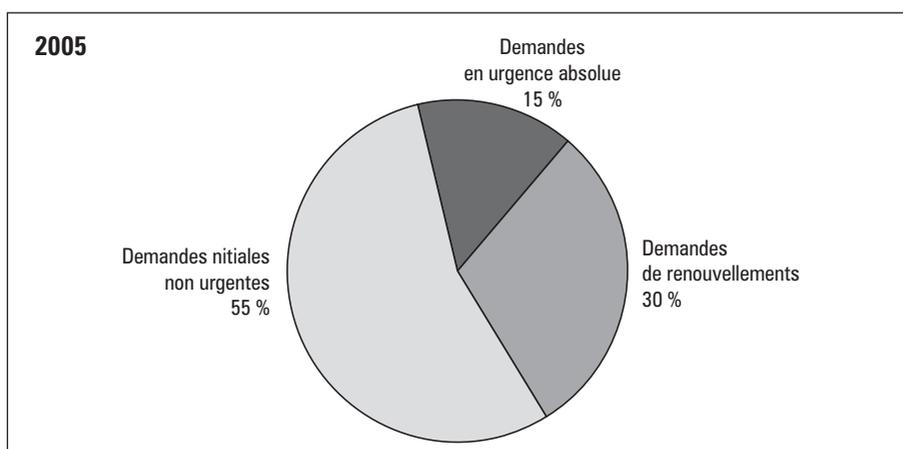
## État comparatif sur cinq ans

Motifs	2002	2003	2004	2005	2006
Sécurité nationale	539	663	629	624	735
Potentiel scientifique et économique	3	22	36	42	28
Terrorisme	814	782	1 052	848	794
Criminalité organisée	216	210	201	182	243
Groupements dissous	0	0	0	1	9
<b>Totaux</b>	<b>1 572</b>	<b>1 677</b>	<b>1 918</b>	<b>1 707</b>	<b>1 809</b>

## 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 renouvellements	
Année 2005	Année 2006	Année 2005	Année 2006	Année 2005	Année 2006
3 290	3 489	854	714	1 738	1 825

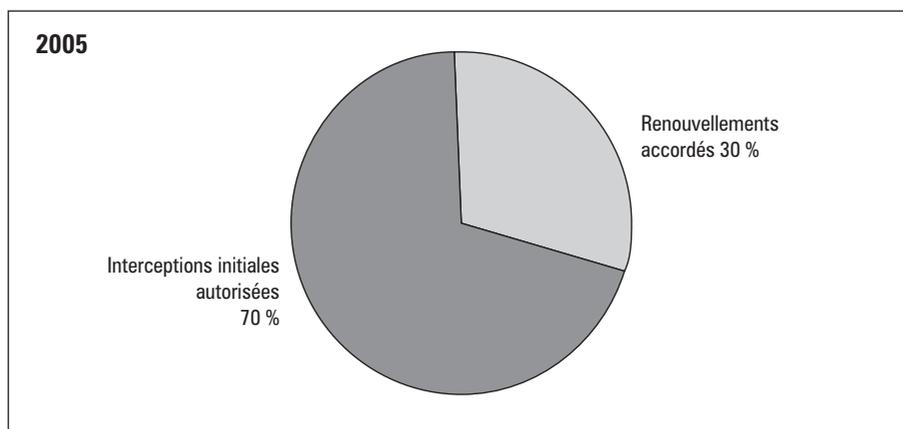
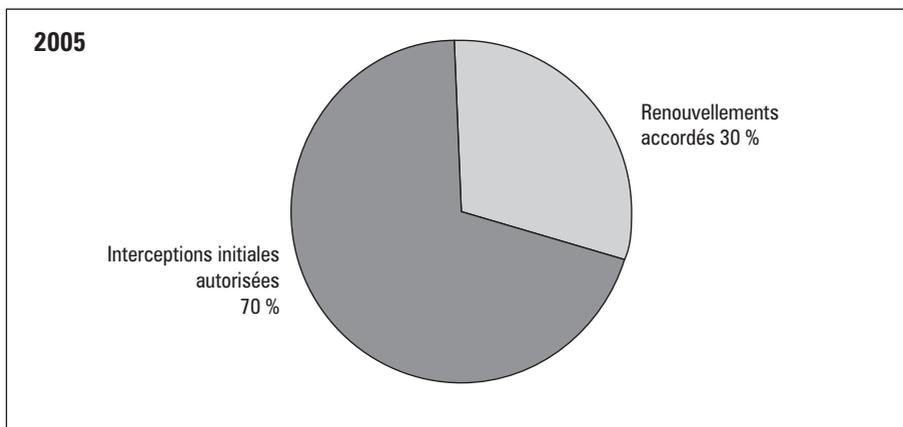


**Demandes d'interceptions : tableau récapitulatif global sur cinq ans**

Type de demandes	2002	2003	2004	2005	2006
Demandes initiales d'interceptions	2 775	2 814	3 154	3 290	3 489
Urgence absolue	363	548	633	854	714
Demandes de renouvellements	1 629	1 677	1 936	1 738	1 825
<b>Total</b>	<b>4 767</b>	<b>5 039</b>	<b>5 723</b>	<b>5 882</b>	<b>6 028</b>

**Répartition entre interceptions et renouvellements accordés****Interceptions accordées en 2006**

Interceptions initiales	Renouvellements	Total
<b>4 176</b>	<b>1 809</b>	<b>5 985</b>



---

# Le contrôle de l'exécution

Celui-ci porte sur trois domaines : en premier lieu l'enregistrement, la transcription et la durée des interceptions ; en second lieu les visites sur le terrain ; enfin et accessoirement, 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 9 de la loi, s'est traduite par un gain de temps appréciable pour les agents chargés de l'exploitation. Cette évolution logicielle ne dispense cependant pas de l'accomplissement des formalités prévues par le deuxième alinéa de l'article 9 : « Il est dressé procès-verbal de cette opération [de destruction des enregistrements à l'expiration d'un délai de 10 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 ses établissements.

Les transcriptions doivent être détruites, conformément à l'article 12 de la loi du 10 juillet 1991, dès que leur conservation n'est plus « indispensable » à la réalisation des fins mentionnées à l'article 3. Même si l'article 12 n'édicte pas de délai, le GIC pour être en conformité avec l'esprit de la loi, édite automatiquement à l'expiration d'un délai de quatre mois un procès-verbal de destruction avalisé par le service compétent qui indique expressément les rares transcriptions qu'il a retenu à l'expiration de ce délai. Un nouveau procès-verbal relatif à ce reliquat est systématiquement édité à nouvelle échéance de quatre mois.

## 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 11<sup>e</sup> 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 4 de la loi du 10 juillet 1991 (« le Premier ministre organise la centralisation de l'exécution des interceptions autorisées »).

Ce service s'adapte constamment 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, 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 sécurité souhaitées par la Commission. Cette phase est à ce jour achevée mais le maillage du territoire en antennes secondaires se poursuit attestant, après la nécessaire étape de restructuration centralisée, de la volonté de donner aux services enquêteurs la proximité attendue.

## Les visites sur le terrain

Comme de coutume la CNCIS a poursuivi son action sur le terrain sous la forme de 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 8 de la loi) et des procès-verbaux de destruction des enregistrements et des transcriptions (articles 9 et 12 de la loi).

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

Au total, sous une forme ou sous une autre, sept visites de services intéressant les régions Haute-Normandie, Midi-Pyrénées et Île-de-France, ont été effectuées. À chaque fois les représentants de la CNCIS dressent un inventaire des pratiques et procédures mises en œuvre par les services pour l'application de la loi du 10 juillet 1991, apportent les informations et éclaircissements utiles, notamment sur le rôle de la CNCIS, recueillent les observations des personnels rencontrés sur les matériels et logiciels mis à leur disposition et s'informent des réalités locales se rapportant aux motifs légaux des interceptions.

## Réclamations de particuliers et dénonciation à l'autorité judiciaire

### Les saisines de la CNCIS par les particuliers

Cette année cinquante-neuf 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 trois fois 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 ; il a également permis de réorienter les demandeurs vers les services ou autorités compétents.

Plusieurs questions ont eu trait à l'écoute et l'enregistrement des conversations téléphoniques sur le lieu de travail. Il est utile sur ce point de se référer aux informations que livre la CNIL sur son site web ([www.cnil.fr](http://www.cnil.fr)) rubriques : approfondir – travail qui peuvent être synthétisées comme suit :

- aucune écoute ou enregistrement permanents des personnels d'une entreprise ou d'une administration ne peut être mis en œuvre sauf législation ou réglementation particulière l'imposant (exemple : passage d'ordres en salles de marchés) ;
- les écoutes ou enregistrements ponctuels ne sont possibles que dans des cas limités et justifiés (formation du personnel à l'accueil téléphonique par exemple) ;
- l'article L. 120-2 du Code du travail dispose que nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature des tâches à accomplir ni proportionnées au but recherché. L'article L. 121-8 du même Code dispose également qu'aucune information concernant directement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance.

En conséquence les instances représentatives du personnel (relevant du Code du travail ou des trois fonctions publiques) doivent être consultées avant toute mise en œuvre de dispositifs d'écoute ou d'enregistrement des conversations téléphoniques (*cf.* notamment article L. 432-2-1 du Code du travail) et le dispositif doit faire l'objet d'une déclaration à la CNIL. Les employés doivent être informés (dispositif d'alerte visuelle et/ou sonore) que leurs conversations sont enregistrées et l'information des interlocuteurs doit être également assurée (message en début d'appel).

S'agissant des courriers adressés à la CNCIS il leur est immédiatement donné suite et il est notifié au requérant conformément à l'article 17 de la loi, que « la Commission a procédé aux vérifications nécessaires ». On relève à ce propos dans les débats parlementaires précédant l'adoption de la loi de 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 »] peut sembler insatisfaisante mais il est difficile 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 en violation de l'article premier du projet de loi par une personne privée ;
- absence de toute interception.

On comprendra aisément au vu de ces différentes hypothèses que la Commission nationale 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 natures confidentielles. « (Assemblée nationale, rapport n° 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 qui entoure les interceptions 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 qui pourrait être révélée à l'occasion de ce contrôle (*cf. infra*).

Pour être complet signalons que :

1) la Commission d'accès aux documents administratifs (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 des communications téléphoniques d'un requérant ;

2) le Conseil d'État dans un arrêt du 28 juillet 1999 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 17 alinéa 2**

Au cours de l'année 2006, la CNCIS n'a pas eu à user des dispositions du 2<sup>e</sup> alinéa de l'article 17 de la loi du 10 juillet 1991 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 15 ».

---

## Le contrôle du matériel

L'année 2006 a permis d'observer le changement d'économie juridique du « contrôle du matériel » (*cf.* rapport 2005 p. 31). Ce nouveau régime, issu de l'arrêté du 29 juillet 2004, participe d'une évolution de l'appréhension de ce secteur d'activité sensible par la puissance publique (*cf.* rapport 2004 p. 34 à 38 – rapport 2005 p. 31 à 33).

Ce régime, traduisant une vision libérale quant à la mise sur le marché d'appareils dont la liste initiale a été réduite et une logique de vigilance quant à leur utilisation finale (*cf.* rapport d'activité 2004 p. 38), a eu un effet immédiat de diminution du nombre de décisions rendues par la Commission consultative compétente pour donner son avis sur les demandes d'acquisition, de détention ou de commercialisation des matériels visés par les articles R. 226-3 et R. 226-7 dans la mesure où les règles de commercialisation ont été allégées par le nouveau dispositif réglementaire.

Cette facilitation de l'accès au marché n'a pas pour autant induit une inflexion dans la qualification du caractère « sensible » de ce type de matériel par les pouvoirs publics.

Ainsi le décret 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 en 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 extra-communautaire) 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'art. R. 226-2 du Code pénal s'est réunie six fois en 2006. Sa composition est la suivante :

- le secrétaire général de la défense nationale 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 de la Commission nationale de contrôle des interceptions de sécurité;
- un représentant de l'Agence nationale des fréquences;
- deux personnalités désignées en raison de leur compétence par le Premier ministre.

La Commission a rendu, en 2006, 549 décisions ventilées comme suit :

- 315 décisions d'autorisation initiale;
- 115 décisions de renouvellement d'autorisation;
- 14 décisions d'ajournement;
- 3 décisions de refus ou de retrait;
- 102 décisions de mise « hors champ » de l'examen pour autorisation.

On relèvera cette année encore (*cf.* rapport d'activité 2005 p. 32) l'importance du nombre de décisions de « mise hors champ » de l'examen de la Commission. Ce mouvement traduit la mise en œuvre de l'arrêté précité qui emporte l'exclusion de certains types de matériels jusqu'alors soumis à autorisation.

Parmi ces équipements, citons les enregistreurs qui ont représenté 59 des 102 cas de mise « hors champ » et les appareils de test et de mesure pour 35 de ce même total de 102 décisions (soit pour ces deux types de matériels 94 décisions sur les 102 considérées).

La CNCIS a également participé aux réunions où certains services de l'État, titulaires d'autorisation de « plein droit » conformément à l'article R. 226-9 du Code pénal, sont invités selon le régime mis en place en 2001 (*cf.* rapport d'activité 2001 p. 27) à produire leurs registres et à décrire leurs règles internes de gestion des matériels sensibles. Ces rencontres permettent aux représentants de la CNCIS de s'assurer du respect des règles adoptées et de l'adéquation des matériels détenus avec les missions confiées à ces services.

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

- *Les textes 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 secrétaire général de la défense nationale, pièce de la procédure d'autorisation est décrite par ce dispositif (article R. 226-2 du Code pénal).

• *L'arrêté du 29 juillet 2004* (cf. *rapport d'activité 2004 p. 35 à 38*) *fixant la liste des appareils soumis à autorisation ministérielle pour application de l'article 226-3 du Code pénal.*

Ce dispositif normatif a été enrichi par deux textes au cours de l'année 2006 :

– l'arrêté du 16 août 2006 mettant en œuvre 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 ».

Ces deux textes sont reproduits ci-après.

**Décrets, arrêtés, circulaires**  
**Textes généraux**  
**Premier ministre**

Arrêté du 16 août 2006 relatif au registre visé par l'article R. 226-10 du Code pénal

NOR : PRMX0609553A

Le Premier ministre,

Vu le Code pénal, notamment les articles R. 226-1 et R. 226-3 et suivants ;

Vu le décret n° 78-78 du 25 janvier 1978 fixant les attributions du secrétaire général de la défense nationale, notamment l'article 7-1 ;

Vu l'arrêté du 29 juillet 2004 fixant la liste d'appareils prévu par l'article R. 226-3 du Code pénal ;

Vu les arrêtés du 2 juin 2005 portant délégation de signature ;

Vu l'avis de la commission consultative chargée d'émettre un avis relatif à l'acquisition, la détention et la commercialisation des appareils susceptibles de porter atteinte à l'intimité de la vie privée ou au secret des correspondances en date du 23 mai 2006 ;

*Arrête :*

**Article 1**

Le registre prévu à l'article R. 226-10 du Code pénal retraçant l'ensemble des opérations relatives aux matériels dont la liste est fixée par l'arrêté du 29 juillet 2004 susvisé est conforme au modèle figurant en annexe du présent arrêté.

**Article 2**

Ce registre revêt la forme d'un cahier coté et paraphé tenu par le responsable de la société qui a souscrit l'engagement de se soumettre aux contrôles nécessaires tel qu'il est prévu à l'article R. 226-4 du Code pénal.

**Article 3**

L'arrêté du 15 janvier 1998 ayant le même objet est abrogé.

**Article 4**

Le présent arrêté sera publié au Journal officiel de la République française.

Fait à Paris, le 16 août 2006.

Pour le Premier ministre et par délégation :  
Le secrétaire général de la défense nationale

**Décrets, arrêtés, circulaires**  
**Textes généraux**  
**Premier ministre**

Instruction du 5 septembre 2006 relative à la commercialisation et à l'acquisition ou détention des matériels permettant de porter atteinte à l'intimité de la vie privée ou au secret des correspondances

NOR : PRMX0609559J

*Introduction*

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 ou de vente (article R. 226-3) et d'acquisition et de détention (article R. 226-7) de matériels permettant de porter atteinte à l'intimité de la vie privée ou au secret des correspondances.

Pour des raisons de compatibilité avec le droit communautaire, la liste d'appareils prévue par l'article 226-3 du Code pénal a été récemment modifiée par l'arrêté du Premier ministre du 29 juillet 2004, en application de l'article R. 226-1 du Code pénal. Elle diffère selon qu'il s'agit de la commercialisation ou de simple acquisition ou détention.

L'article 7-1 du décret du 25 janvier 1978 modifié relatif aux attributions du SGDN dispose que « Le secrétaire général de la défense nationale instruit les demandes d'autorisation présentées en application de l'article 226-3 du Code pénal. Il préside la commission chargée d'émettre un avis sur ces demandes d'autorisation ».

Par arrêtés du 2 juin 2005 (*Journal officiel* du 3 juin 2005), délégation est donnée au secrétaire général de la défense nationale pour signer, au nom du Premier ministre, les autorisations, refus ou retraits d'autorisation (articles R. 226-3 et R. 226-7 du Code pénal) et les arrêtés.

La présente instruction a pour but de préciser les modalités des procédures d'examen des demandes, la compétence de la commission consultative chargée de soumettre un avis au Premier ministre ainsi que le rôle des différents services chargés de fournir des avis techniques et de moralité.

#### **Article 1<sup>er</sup>** – Instruction des demandes

L'article R. 226-4 du Code pénal dispose que la demande d'autorisation pour la fabrication, l'importation, l'exposition, l'offre, la location ou la vente de tout appareil figurant sur la liste mentionnée à l'article R. 226-1 est déposée auprès du secrétaire général de la défense nationale.

L'article R. 226-8 du Code pénal dispose que la demande d'autorisation pour l'acquisition ou la détention de tout appareil figurant sur la liste mentionnée à l'article R. 226-1, est déposée auprès du secrétaire général de la défense nationale (SGDN).

Toute demande d'autorisation doit être adressée à la direction « protection et sécurité de l'État » du SGDN, qui en assure l'instruction.

1 – Les dossiers concernant les demandes d'autorisation pour la fabrication, l'importation, l'exposition, l'offre, la location ou la vente (article R. 226-3) doivent comporter, pour chaque type d'appareil (article R. 226-4) :

1°) le nom et l'adresse du demandeur, s'il est une personne physique, ou sa dénomination et son siège s'il est une personne morale ;

2°) la ou les opérations mentionnées à l'article R. 226-3 pour lesquelles l'autorisation est demandée et la description des marchés visés ;

3) l'objet et les caractéristiques techniques du type de l'appareil, accompagnés d'une documentation technique détaillée décrivant :

– les capacités à capter, enregistrer ou transmettre, sans le consentement de leurs auteurs, des paroles prononcées à titre privé ou confidentiel ;

– les moyens éventuels de cryptologie intégrés ou intégrables dans le matériel ;

– les moyens et méthodes permettant de prévenir l'usage non autorisé du matériel ;

4°) le lieu prévu pour la fabrication de l'appareil ou pour les autres opérations mentionnées à l'article R. 226-3. En cas d'importation, l'appellation du produit d'origine, son appellation commerciale et son lieu de fabrication ;

5°) l'engagement de se soumettre aux contrôles nécessaires à la vérification du respect des indications fournies dans la demande d'autorisation. Afin de vérifier le lien effectif entre le signataire de l'acte d'engagement et la société à l'origine de la demande, un extrait K bis de moins d'un mois complètera le dossier.

L'autorisation mentionnée à l'article R. 226-3 est délivrée pour une durée maximale de six ans.

2 – Les dossiers concernant les demandes d'autorisation pour l'acquisition ou la détention (article R. 226-7) doivent comporter pour chaque type d'appareil (article R. 226-8) :

1°) le nom et l'adresse du demandeur, s'il est une personne physique, ou sa dénomination et son siège s'il est une personne morale ;

2°) l'objet et les caractéristiques techniques du type de l'appareil, accompagnés d'une documentation technique détaillée décrivant :

– les capacités à capter, enregistrer ou transmettre, sans le consentement de leurs auteurs, des paroles prononcées à titre privé ou confidentiel ;

– les moyens éventuels de cryptologie intégrés ou intégrables dans le matériel ;

– les moyens et méthodes permettant de prévenir l'usage non autorisé du matériel ;

3°) le nombre d'appareils pour la détention desquels l'autorisation est demandée ;

4°) l'utilisation prévue et son cadre d'emploi ;

5°) L'engagement de se soumettre aux contrôles nécessaires à la vérification du respect des indications fournies dans la demande d'autorisation.

L'autorisation mentionnée à l'article R. 226-7 est délivrée pour une durée maximale de trois ans.

*Remarques :* la location et la détention de matériel peuvent s'inscrire dans le cadre d'une enquête préliminaire ou de flagrance ou d'une commission rogatoire d'un juge d'instruction. Dans ce cas, la réquisition vaut autorisation pour l'utilisateur.

Chaque cession, transfert, location ou vente de matériel ne pourra être effectué qu'après autorisation, tant en ce qui concerne le vendeur que le nouvel acquéreur (article R. 226-10), en fonction du type des matériels visés dans la liste annexée à l'arrêté du 29 juillet 2004.

En outre, il convient de souligner que l'autorisation du Premier ministre ne dispense pas son bénéficiaire, pour la mise sur le marché, du respect d'autres réglementations, en particulier celles relatives à l'évaluation de conformité des équipements terminaux de télécommunications, à l'utilisation de fréquences radioélectriques, à l'importation des matériels de guerre et à l'utilisation de dispositifs de cryptologie.

#### **Article 2 – Compétence de la commission consultative**

La commission consultative, dont la composition figure en annexe, est chargée d'assister le Premier ministre et notamment d'émettre un avis sur les différentes demandes d'autorisation qui lui sont présentées, après recueil des avis technique et de moralité.

Elle est présidée par le SGDN et se réunit périodiquement à l'initiative de son président qui en fixe l'ordre du jour.

La commission émet un avis sur :

##### 1) Les demandes d'autorisation et de renouvellement de plein droit

Conformément aux termes du troisième alinéa de l'article R. 226-9, l'autorisation mentionnée à l'article R. 226-7 du Code pénal (acquisition ou détention) de tout appareil figurant en annexe de l'arrêté du 29 juillet 2004 est accordée de plein droit aux agents ou services de l'État habilités à réaliser des interceptions autorisées par la loi, après avis de la commission consultative réunie dans son format restreint.

Le SGDN s'assure que la demande d'autorisation est accordée aux agents ou services de l'État habilités à réaliser des interceptions autorisées par la loi et il en informe la commission consultative.

##### 2) Les demandes d'autorisation et de renouvellement

Les dossiers de demandes d'autorisation se répartissent en deux catégories conformément aux articles R. 226-3 et R. 226-7 du Code pénal.

« Article R. 226-3. – Les demandes concernant la fabrication, l'importation, l'exposition, l'offre, la location ou la vente de tout appareil figurant en annexe de l'arrêté du 29 juillet 2004. »

« Article R. 226-7. – Les demandes concernant l'acquisition ou la détention de tout appareil figurant en annexe de l'arrêté du 29 juillet 2004. »

Les demandes de renouvellement sont également soumises à la commission et sont effectuées trois mois avant la fin de la validité de l'autorisation en cours.

En cas de demande de renouvellement hors délais, la nouvelle autorisation prend effet à compter de la date de sa délivrance et sans effet rétroactif.

##### 2 bis) L'exposition

L'exposition des matériels soumis à autorisation est exclusivement limitée auprès des personnes, services de l'État ou entreprises titulaires d'une autorisation d'acquisition ou de détention

du matériel exposé. Elle ne permet pas la vente d'un matériel, sauf si l'autorisation signée par le secrétaire général de la défense nationale le précise.

### 3) Les contrôles

En vertu des articles R. 226-4 (5°) et R. 226-8 (4°) du Code pénal, le bénéficiaire d'une autorisation est tenu de se soumettre, conformément à l'acte d'engagement qu'il a signé, aux contrôles nécessaires à la vérification du respect des indications fournies dans la demande d'autorisation.

Ces contrôles concernent notamment le registre, dont le modèle est défini par l'arrêté du 16 août 2006, qui retrace l'ensemble des opérations relatives aux matériels. Le bénéficiaire d'une autorisation doit permettre l'accès aux matériels, à la description précise de la configuration matérielle et logicielle mise en place et à la documentation technique détaillée (caractéristiques techniques, exploitation, maintenance locale et à distance, sécurisation des dispositifs incluant selon le cas l'authentification, la confidentialité, la traçabilité et l'intégrité).

Les contrôles peuvent être effectués, tout d'abord, lors du dépôt d'une demande d'autorisation puis, d'une façon inopinée, durant toute la durée de validité de l'autorisation accordée.

### 4) Des arrêtés

La commission consultative est saisie pour avis des projets d'arrêtés pris en application des articles R. 226-1 et R. 226-10 du Code pénal. Elle peut formuler des propositions de modification de ces arrêtés.

## **Article 3 – Conditions d'octroi des avis techniques et de moralité**

### 1) Les conditions d'octroi de l'avis technique

Chaque demande est adressée par le SGDN au laboratoire technique désigné par le Premier ministre, pour avis technique. Selon le cas, un autre membre de la commission peut également être destinataire de la demande.

Le laboratoire technique examine la notice technique de l'appareil objet de la demande et se rend en tant que de besoin sur place ou teste l'ensemble dans ses ateliers pour constater la conformité du matériel. Il peut saisir le ministère chargé des communications électroniques. Lorsque l'appareil comporte un émetteur radioélectrique, il saisit l'Agence nationale des fréquences avant de transmettre au SGDN un avis sans objection ou un avis défavorable motivé.

Les ministères de l'Intérieur et de la Défense adresseront un avis technique au SGDN chaque fois qu'ils le jugeront nécessaire.

Un examen de la conformité avec l'usage déclaré du matériel peut être diligenté afin de s'assurer que :

- la déclaration est conforme aux caractéristiques du matériel ;
- les fonctionnalités du matériel correspondent à l'usage déclaré.

### 2) Les conditions d'octroi des avis de moralité

Chaque demande est également adressée par le SGDN au ministère de la Justice, au ministère de l'Intérieur (DGPN), au ministère de la Défense (cabinet) et au ministère du Budget (direction générale des douanes). Les avis de moralité sont de la compétence :

- A) du ministère de la Justice : son représentant fait connaître, lors de la réunion de la commission consultative, les éventuelles observations qu'appellent les différentes demandes d'autorisation présentées ;
- B) de la direction générale des douanes : la direction nationale du renseignement et des enquêtes douanières fait connaître au SGDN, lors de la réunion de la commission consultative, les éventuelles observations qu'appellent les différentes demandes d'autorisation présentées ;
- C) du ministère de l'Intérieur : après enquête, la DGPN adresse au SGDN un avis sans objection ou un avis défavorable motivé dans le délai d'un mois ;

D) du ministère de la Défense : après enquête, le ministère de la défense adresse au SGDN un avis sans objection ou un avis défavorable motivé dans le délai d'un mois.

### 3) Avis des membres de la commission consultative

Le SGDN adresse aux membres de la commission consultative la liste des nouvelles demandes pour leur permettre, lors de chaque réunion, de formuler leurs observations.

### Article 4 – Retraits d'autorisation

L'article R. 226-11 du Code pénal prévoit la possibilité de retirer les autorisations dans des cas strictement énumérés. Sauf urgence, le retrait ne peut intervenir qu'après que le titulaire de l'autorisation a été mis à même de faire valoir ses observations.

Le Premier ministre peut, lorsqu'il envisage de prononcer le retrait d'autorisations, consulter la commission instituée par l'article R. 226-2 du même Code.

On peut classer ces retraits en deux catégories.

A) Le retrait administratif de l'autorisation lié au non-respect des dispositions législatives ou réglementaires :

Aux termes de l'article R. 226-11 du Code pénal, le Premier ministre, après instruction du dossier par le SGDN, peut retirer les autorisations prévues aux articles R. 226-3 et R. 226-7 dans les cas suivants :

- fausse déclaration ou faux renseignement ;
- modification des circonstances au vu desquelles l'autorisation a été délivrée ;
- lorsque le bénéficiaire de l'autorisation cesse l'exercice de l'activité pour laquelle a été délivrée l'autorisation ;
- lorsque le bénéficiaire de l'autorisation n'a pas respecté les dispositions des articles R. 226-1 à R. 226-12 ou les obligations particulières prescrites par l'autorisation.

Ainsi, constitue un motif de retrait :

– s'agissant de l'ensemble des titulaires d'autorisation :

a) le refus de se soumettre aux contrôles nécessaires à la vérification du respect des indications fournies dans la demande d'autorisation (articles R. 226-4 et R. 226-8) ;

b) le non-respect des obligations dont est assortie l'autorisation (articles R. 226-5 et R. 226-9) ;

– s'agissant des titulaires d'une autorisation de fabrication, d'importation, d'exposition, d'offre, de location ou de vente :

a) le fait de ne pas tenir un registre ou de refuser de le présenter aux services enquêteurs (article R. 226-10) ;

b) le fait de ne pas avoir porté, sur chaque appareil fabriqué, importé, exposé, offert, loué ou vendu, la référence du type correspondant à la demande d'autorisation (article R. 226-6) ;

c) le fait d'avoir proposé, cédé, loué ou vendu des appareils à des personnes ou sociétés non autorisées (article R. 226-10) ;

d) le fait de réaliser une publicité en faveur d'un appareil susceptible de permettre la réalisation des infractions prévues par l'article R. 226-1 et le second alinéa de l'article 226-15 du Code pénal lorsque cette publicité constitue une incitation à commettre ces infractions.

B) Le retrait de l'autorisation lié à une condamnation pénale :

Selon les termes de l'article R. 226-11, *in fine*, l'autorisation prend fin de plein droit en cas de condamnation pénale définitive pour l'une des infractions prévues aux articles 226-1, 226-15 et 432-9 du Code pénal. Si tel est le cas, le SGDN avise les membres de la commission et procède à la clôture du dossier.

Le ministre de la Justice, par son représentant, fait connaître au SGDN les condamnations pénales qui mettent fin de plein droit aux autorisations (article R. 226-11 du Code pénal). Le SGDN en informe les membres de la commission consultative.

Lorsque le Premier ministre prend une décision de retrait, copie de cette décision est adressée à la DGPN pour notification à l'intéressé. Les services de police désignés par la DGPN procèdent à la notification de la décision de retrait et invitent la personne concernée à se mettre en conformité avec les termes de l'article R. 226-12. Ils prennent rendez-vous avec l'intéressé pour que celui-ci, dans le délai d'un mois, procède en leur présence à la destruction de l'appareil. Procès-verbal est dressé et copie en est adressée au SGDN par l'intermédiaire de la DGPN. Si la personne concernée décide, comme l'article R. 226-12 lui en laisse la possibilité, de vendre ou de céder l'appareil à une personne disposant d'une autorisation, l'officier de police judiciaire doit, après s'être assuré de la réalité de la vente ou de la cession du matériel, dresser procès-verbal et en adresser une copie selon les mêmes modalités qu'en cas de destruction.

La même procédure est appliquée lorsqu'il apparaît que la personne qui s'est vu opposer un refus était déjà en possession du matériel.

Pour le Premier ministre et par délégation  
Le secrétaire général de la défense nationale

---

# Actualités de l'année 2006

## Le renforcement de la lutte contre le terrorisme : la loi n° 2006-64 du 23 janvier 2006

Cette loi traduit, pour la première fois depuis la création de la CNCIS, une extension des compétences de cette dernière. Conçu dans la foulée des attentats de Londres le projet a été présenté au Parlement comme devant relever, dans un contexte marqué par l'hyperterrorisme, le niveau de sécurité préventive du pays en utilisant les nouvelles possibilités offertes par la technologie ou en trouvant des parades à ces mêmes moyens quand ils sont déjà utilisés par les groupes terroristes.

Plusieurs dispositions de la loi ont concerné plus particulièrement la Commission. La première, indirectement, consistant à assimiler les gérants exploitant de cybercafé à des opérateurs afin de faire peser sur eux des obligations identiques en matière de conservation des données. Cette disposition n'appelle pas de commentaires particuliers. La seconde, la plus importante, ouvre la possibilité d'une surveillance administrative des données d'appel autres que le contenu de ceux-ci et de localisation des terminaux en matière terroriste. Enfin, la *personnalité qualifiée* ainsi que ses *adjoints*, chargés d'administrer les demandes d'accès à ces données ainsi formées par les services habilités, font l'objet d'une désignation pour trois ans, renouvelable, par la Commission. Ces dispositions seront exposées dans le chapitre relatif à l'actualité législative (p. 59).

Il convient de revenir sur la notion de « données d'appel » autrement qualifiée par la Commission de « prestations annexes ».

Rappelons ici que cette notion avait été abordée par la CNCIS dans son rapport d'activité de l'année 1999 (CNCIS 8<sup>e</sup> rapport, p. 30) et développée sur le plan doctrinal par le professeur Truchet dans le numéro du 10<sup>e</sup> anniversaire de la Commission (CNCIS 10<sup>e</sup> rapport p. 69, 70, 76-77).

Au sens strict et conformément à l'article 22 de la loi du 10 juillet 1991, les prestations annexes sont constituées des informations ou documents nécessaires aux juridictions compétentes ou au Premier ministre pour ordonner des interceptions qu'ils peuvent recueillir auprès des exploitants ou fournisseurs de services de réseaux de communications électroniques pour la réalisation et l'exploitation des interceptions autorisées par la loi.

En clair, convient-il d'une part avant de solliciter une interception de sécurité de s'assurer de l'identité de l'abonné, de vérifier si la ligne est active et auprès de quel opérateur et, d'autre part, au stade de l'exploitation de l'interception, d'identifier, notamment par exploitation de la « fadette » (facturation détaillée), les numéros appelants et appelés et de localiser les appels reçus ou émis.

Les services chargés de la lutte contre le terrorisme sont convaincus que ces données sont infiniment plus « parlantes » pour établir la cartographie d'un réseau terroriste que des correspondances échangées aux propos convenus ou codés.

Les services ont donc exprimé le souhait de pouvoir exploiter les seules données de signalisation dans des délais plus rapides que ceux requis pour l'autorisation et la mise en place des interceptions.

Le projet de la loi élaboré à l'automne a ainsi ouvert la possibilité aux agents habilités des services de police et de gendarmerie de requérir les opérateurs de communications électroniques pour obtenir ces prestations qui dans cette hypothèse ne peuvent plus porter le nom d'annexes.

Dans le cas des prestations annexes, le contrôle de la Commission s'exerçait par le haut c'est-à-dire qu'il était compris dans celui portant sur l'interception.

Dans l'hypothèse d'un accès des services à des prestations non liées à une interception et quand bien même celles-ci ne constituent pas des correspondances au sens strict, des modalités de contrôle devaient nécessairement être envisagées puisque, selon les initiateurs du projet, le « contenant » renseigne parfois plus que le « contenu » sur la vie privée.

Deuxième partie

---

# ÉTUDES ET DOCUMENTS

---

# Présentation ordonnée des textes relatifs aux interceptions

Les modifications législatives et réglementaires intervenues dans le domaine de l'interception et de surveillance des correspondances transmises par la voie des « communications électroniques » courant 2005 et 2006 rendent nécessaire leur présentation actualisée et exhaustive.

Avant de reproduire les 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 1<sup>er</sup> de la loi n° 91-646 du 10 juillet 1991 : « 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'intervention des lois n° 2002-1138 du 9 septembre 2002 et 2004-204 du 9 mars 2004.

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 :

- article 74-2 du même Code (recherche d'une personne en fuite);
- article 80-4 du même Code (recherche des causes de la mort ou d'une disparition présentant un caractère inquiétant);
- article 706-95 du même Code (criminalité et délinquance organisées).

On trouvera ci-dessous le tableau récapitulatif des différents types d'interceptions judiciaires et de sécurité.

**Tableau récapitulatif des durées d'interceptions et conditions de renouvellement**

	<b>Autorité</b>	<b>Motif</b>	<b>Durée</b>	<b>Renouvellement</b>
Interceptions de sécurité	Premier ministre (article 3, loi du 10 juillet 1991)	Prévention – terrorisme – criminalité organisée – sécurité nationale – protection économique – ligues dissoutes	4 mois	Sans limitation
Interceptions judiciaires	Juge d'instruction (article 100 Code de procédure pénale)	Matière criminelle et correctionnelle (peine encourue supérieure à 2 ans)	4 mois	Sans limitation
	Juge d'instruction (article 80-4 Code de procédure pénale)	Recherche des causes de la mort ou de disparitions inquiétantes	2 mois	Sans limitation
	Parquet sous l'autorité du juge des libertés et de la détention (article 74-2-695-36 et 696-21 Code de procédure pénale)	Recherche de personnes en fuite	2 mois	Renouvelable 3 fois en matière correctionnelle; sans limitation en matière criminelle
	Parquet (sous l'autorité du juge des libertés et de la détention) (article 706-95 Code de procédure pénale)	Criminalité organisée	15 jours	Renouvelable une fois

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 font pas strictement partie du Titre I de la loi de 1991.

## Loi n° 91-646 du 10 juillet 1991 (consolidée)

### • TITRE I : DES INTERCEPTIONS ORDONNÉES PAR L'AUTORITÉ JUDICIAIRE

#### **Les interceptions ordonnées en matière criminelle et correctionnelle**

Code de procédure pénale : Livre premier : De l'exercice de l'action publique et de l'instruction;

Titre III : Des juridictions d'instruction;

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

Sous-section 2. Des interceptions de correspondances émises par la voie des télécommunications (loi n° 91-646 du 10 juillet 1991 – Titre I);

**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. »

• Loi n° 2005-1549 du 12 décembre 2005 à peine de nullité, ne peuvent être transcrites les correspondances avec un avocat relevant de l'exercice des droits de la défense.

**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 n° 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**

**Article 74-2** – Code de procédure pénale – « 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 [...] ».

*Nota bene* : 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**

**Article 80-4** – Code de procédure pénale (loi n° 2002 -1138 du 9 septembre 2002, article 66) – « 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 1<sup>er</sup> du Titre III du Livre I. 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**

**Article 706-95** – du Code de procédure pénale – « 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 de quinze jours, 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 [...]. »

### **• TITRE II : DES INTERCEPTIONS DE SÉCURITÉ**

**Article 3** – « Peuvent être autorisées, à titre exceptionnel, dans les conditions prévues par l'article 4, les interceptions de correspondances émises par la voie des "communications électroniques" (loi 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 reconsti-

tution 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 n° 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 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 quarante-huit 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 visés 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 n° 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 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 n° 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 : 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 n° 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 "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 « 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<sup>1</sup> 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 : 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 n° 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 n° 2004-575 du 21 juin 2004 précitée. »

• *TITRE V : DISPOSITIONS FINALES*

**Article 28** – « La présente loi entrera en vigueur le 1<sup>er</sup> octobre 1991. »

---

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

## Textes réglementaires récents visant la loi du 10 juillet 1991

### **Décret n° 2002-497 du 12 avril 2002 relatif au groupement interministériel de contrôle (JO du 13 avril 2002)**

« [...] Vu la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques », modifiée par la loi n° 92-1336 du 16 décembre 1992, l'ordonnance n° 2000-916 du 19 septembre 2000 et la loi n° 2001-1062 du 15 novembre 2001 [...] ».

**Article 1<sup>er</sup>** – « 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 n° 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 n° 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<sup>er</sup>** – « 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 1<sup>er</sup> 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 1<sup>er</sup> :

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*. »

---

# Actualité législative

## 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 plus 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 techni-

ques 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 n° 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 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 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.** A la fin de la seconde phrase du premier alinéa de l'article 4 de la loi n° 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 n° 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 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 n° 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 n° 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. En application de l'article sus-exposé et du décret 2006-1651 du 22 décembre 2006, la Commission a désigné le 26 décembre 2006 Monsieur François Jaspard en qualité de personnalité qualifiée.

- 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 n° 2002-532 DC du 19 janvier 2006). Une séparation nette entre réquisitions judiciaires (*cf.* notamment article 77-1-1 du Code de procédure pénale) et réquisitions administratives (article 22 de la loi du 10 juillet 1991 et 6 de la loi n° 2006-64 du 23 janvier 2006) est ainsi assurée identique à la séparation entre interceptions judiciaires (article 100 à 100-7 du Code de procédure pénale) et interceptions administratives à laquelle la CNCIS a toujours attaché du prix (CNCIS 3<sup>e</sup> rapport, 1994 p. 19; CNCIS 7<sup>e</sup> rapport, 1998 p. 23; CNCIS 8<sup>e</sup> rapport, 1999, p. 14).

- Sur le contrôle des demandes :

Le texte définitivement adopté stipule que par parallélisme avec les procédures de demandes d’interceptions, que 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.

## **Décret n° 2006-1405 du 17 novembre 2006 relatif à l’organisation du ministère de la Justice et instituant une délégation aux interceptions judiciaires**

Cette délégation a pour mission d’animer et de coordonner, dans le cadre d’orientations générales proposées au ministre de la Justice par le Comité d’orientation des interceptions judiciaires, les actions visant à assurer la bonne exécution et la maîtrise financière des opérations d’interceptions de correspondances émises par la voie des communications électroniques, de conservation et de transmission des données relatives aux abonnements souscrits ainsi qu’aux données de connexion, d’identification des correspondants et de localisation des équipements terminaux, pratiquées dans le cadre judiciaire.

La délégation est ainsi chargée de coordonner et d’harmoniser, dans une chaîne allant des enquêteurs aux opérateurs, les dispositifs techniques et procéduraux de mise en œuvre des interceptions et de rémunération des opérateurs requis.

---

# Observations sur les motifs légaux d'interception

Les réflexions de la Commission sur les motifs légaux d'interception ont été successivement présentées dans le 11<sup>e</sup> rapport d'activité (« criminalité organisée » et « terrorisme ») et dans le 12<sup>e</sup> rapport (« sécurité nationale » et « protection économique »). La Commission entend désormais présenter de façon permanente mais plus synthétique ses observations sur ces quatre motifs. Aucun développement ne sera en revanche consacré au cinquième motif « reconstitution ou maintien de groupements dissous » en raison du volume non significatif des interceptions accordées de ce chef.

\*\*\*

## Sécurité nationale

Conformément à l'article 3 de la loi du 10 juillet 1991 « peuvent être autorisées [...] les interceptions [...] ayant pour objet de rechercher des renseignements intéressant la *sécurité nationale* [...] ».

« Sécurité nationale », « sécurité intérieure et extérieure », « sûreté de l'État », « intérêts fondamentaux de la Nation » sont des concepts voisins souvent employés indistinctement, tout au moins pour les trois premiers. En revanche, 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 I du Livre III du Code pénal ».

Article 8 alinéa 2 de la Convention européenne : « 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 liberté d'autrui ».

Les anciens articles, aujourd'hui abrogés, du Code pénal auxquels se référait le Sénat étaient les articles 70 à 103 dont les incriminations se retrouvent globalement dans l'actuel Livre IV du « nouveau » Code pénal, constituant désormais les « atteintes aux intérêts fondamentaux de la nation ».

Les intérêts fondamentaux de la Nation constituent donc 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.

Code pénal, article 410-1 : « 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.

Rapidement (rapport d'activité 1994, p. 17 s.), la CNCIS a estimé que la notion de sécurité nationale devait bien être comprise au vu des dispositions du Nouveau Code pénal qui fait figurer cette notion parmi les intérêts fondamentaux de la Nation (article 410-1 du Code pénal) au même titre que l'intégrité du territoire, la forme républicaine des institutions ou les 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 ainsi estimé utile de rappeler 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 au sens ci-dessus rappelé».

On relève dans le même rapport (p. 36) que :

- «la crainte d'un trouble à l'ordre public n'autorise le recours à une interception qu'en cas de menace particulièrement grave à la sécurité ;
- «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».

La Commission est restée fidèle à cette doctrine.

- S'agissant des troubles à l'ordre public, des demandes motivées par cette crainte peuvent parfois être présentées sans que soit cependant allégué le risque d'attenter à la forme républicaine des institutions ou de déboucher sur un mouvement insurrectionnel. Si des manifestations sont susceptibles de dégénérer, le droit de manifester étant constitutionnellement reconnu, il s'agit là, en principe, 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 la charge symbolique voulue par leurs auteurs affectant le lieu et le temps des manifestations, la qualité des autorités ou des symboles visés, sont tels que la sécurité intérieure peut être menacée.

- S'agissant de la recherche de renseignements sur la situation politique prévalant dans un pays tiers, la personne dont on se propose d'intercepter les correspondances doit être suspectée d'attenter par ses agissements 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 la palette des sources disponibles, les interceptions de sécurité doivent faire exception. En effet, l'atteinte exceptionnelle à la vie privée qu'autorise la loi ne peut être justifiée 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 au principe de proportionnalité et l'avis de la Commission ne pourrait être que défavorable. Cette observation vaut naturellement pour les autres motifs légaux d'interception comme la prévention du terrorisme et la lutte contre la criminalité organisée même si, pour ces derniers, l'implication de la cible dans le processus conspiratif ou criminel est en principe avérée.

Enfin, la Commission entend opérer une appréciation *in concreto* de la notion « d'intérêts fondamentaux de la Nation », la notion de sécu-

rité étant appréhendée en un instant donné et dans un contexte géopolitique donné par rapport aux besoins vitaux du pays.

## Sauvegarde du potentiel scientifique et économique de la Nation

La sauvegarde des **éléments essentiels du potentiel scientifique et économique de la France**, plus communément et rapidement nommée « protection économique », est, à l'exception de la reconstitution de ligues dissoutes le motif d'interception le plus faible en volume, bien qu'il connaisse un certain renouveau suite au développement de la réflexion politique et à la mise en place de structures concernant « l'intelligence économique ».

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 selon eux « fourretout » de ces motifs (Assemblée nationale 2<sup>e</sup> séance 13 juin 1991, *JO*, p. 3153; Sénat du 25 juin 1991 *JO*, p. 2065), ont obtenu que la rédaction s'inspire de celle envisagée au Livre IV du Code pénal pour décrire les intérêts fondamentaux de la nation alors en gestation. L'article 410-1 qui ouvre le Livre IV du Code pénal vise effectivement la « sauvegarde des éléments essentiels du potentiel scientifique et économique [de la Nation] ».

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 Convention européenne des droits de l'homme, dont le texte est d'ailleurs moins restrictif que le projet de loi, puisqu'il se réfère à la notion de "bien-être économique" (cf. *supra* p. 64) » [...] 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, document n° 2088, p. 29).

« 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 » (A. Vitu, article 410-1 et suivants *Jurisclasseur pénal*).

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 : est en effet visée, notamment, 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<sup>1</sup> ou organisations étrangères.

Un exemple, bien évidemment déconnecté de tout dossier réel, permettra de mieux illustrer la légitimité d'une demande d'interception de sécurité formulée dans un contexte d'espionnage économique.

Une personne est suspectée de recueillir en vue de leur transfert illicite des secrets de fabrication d'un groupe français leader mondial dans sa spécialité.

Le transfert illicite d'un secret de fabrication à une entité étrangère permet d'établir la réunion de plusieurs éléments constitutifs des délits de l'art. 411-7 du Code pénal (on peut d'ailleurs noter que « la communication de secret de fabrication » était déjà incriminée par l'ancien article 418).

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 comme l'est le faux en écriture, acte préparatoire d'une éventuelle escroquerie), sont réunis et l'interception de sécurité parfaitement fondée en droit.

Il résulte de ce qui précède 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 direc-

1) Le terme entreprise étant ici entendu non au sens « d'entreprise terroriste » comme dans l'article 421-1 du Code pénal, mais bien au sens du droit commercial du droit du travail et de l'économie politique à savoir la réunion des facteurs de production du capital et du travail nécessaires à la mise en œuvre d'une activité professionnelle déterminée.

tement reprise du Code pénal et renvoie à des infractions précises, doivent d'une part répondre à une suspicion d'atteinte à ce potentiel, une menace réelle sur les recherches en cours, les brevets, le *know how*, etc. et que, d'autre part, la personne dont il est demandé d'intercepter les communications doit être clairement impliquée dans cette menace.

Il convient par ailleurs de constater que les pouvoirs publics proposent une approche normative des intérêts économiques et scientifiques constituant une forme de « noyau dur » à protéger prioritairement.

Ainsi, le décret 2005-1739 du 30 décembre 2005 *réglementant les relations financières avec l'étranger* [...] est venu définir en ses articles 2 et 3 (reproduits ci-après) 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 ».

Articles 2 et 3 du décret du 30 décembre 2005 :

Chapitre I<sup>er</sup>  
Dispositions relatives aux investissements étrangers  
en provenance de pays tiers

**Article 2** – Il est inséré au chapitre III du Titre V du Livre I du même Code une section 1 ainsi rédigée :

*« Section 1  
« Dispositions relatives aux investissements étrangers  
en provenance de pays tiers*

**Article R. 153-1** – Constitue un investissement au sens de la présente section le fait pour un investisseur :

- « 1°) soit d'acquérir le contrôle, au sens de l'article L. 233-3 du Code de commerce, d'une entreprise dont le siège social est établi en France ;
- « 2°) soit d'acquérir directement ou indirectement tout ou partie d'une branche d'activité d'une entreprise dont le siège social est établi en France ;
- « 3°) soit de franchir le seuil de 33,33 % de détention directe ou indirecte du capital ou des droits de vote d'une entreprise dont le siège est établi en France.

**Article R. 153-2** – Relèvent d'une procédure d'autorisation au sens du I de l'article L. 151-3 les investissements étrangers mentionnés à l'article R. 153-1 réalisés par une personne physique ressortissante d'un État non-membre de la Communauté européenne, par une entreprise dont le siège social se situe dans l'un de ces mêmes États ou par une personne physique de nationalité française qui y est résidente, dans les activités suivantes :

- « 1°) activités dans les secteurs des jeux d'argent ;
- « 2°) activités réglementées de sécurité privée ;
- « 3°) activités de recherche, de développement ou de production relatives aux moyens destinés à faire face à l'utilisation illicite, dans le cadre d'activités terroristes, d'agents pathogènes ou toxiques et de prévenir les conséquences sanitaires d'une telle utilisation ;
- « 4°) activités 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 ;

«5) activités de services dans le cadre de centres d'évaluation agréés dans les conditions prévues au décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information ;

«6°) activités de production de biens ou de prestation de services de sécurité dans le secteur de la sécurité des systèmes d'information d'une entreprise liée par contrat passé avec un opérateur public ou privé gérant des installations au sens des articles L. 1332-1 à L. 1332-7 du Code de la défense ;

«7°) activités relatives aux biens et technologies à double usage énumérés à l'annexe IV du règlement (CE) n° 1334/2000 du Conseil du 22 juin 2000 modifié instituant un régime communautaire de contrôle des exportations de biens et technologies à double usage ;

«8°) activités relatives aux moyens de cryptologie et les prestations de cryptologie mentionnés aux paragraphes III, IV de l'article 30 et I de l'article 31 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;

«9°) activités exercées par les entreprises dépositaires de secrets de la défense nationale notamment au titre des marchés classés de défense nationale ou à clauses de sécurité conformément au décret n° 98-608 du 17 juillet 1998 relatif à la protection des secrets de la défense nationale ;

«10°) activités de recherche, de production ou de commerce d'armes, de munitions, de poudres et substances explosives destinées à des fins militaires ou de matériels de guerre et assimilés réglementés par le Titre III ou le Titre V du Livre III de la deuxième partie du Code de la défense ;

«11°) activités exercées par les entreprises ayant conclu un contrat d'étude ou de fourniture d'équipements au profit du ministère de la défense, soit directement, soit par sous-traitance, pour la réalisation d'un bien ou d'un service relevant d'un secteur mentionné aux points 7°) à 10°) ci-dessus. »

## Chapitre II

### Dispositions relatives aux investissements en provenance des États membres de la Communauté européenne

**Article 3** – Il est inséré au chapitre III du Titre V du Livre I du même Code une section 2 ainsi rédigée :

#### *« Section 2*

#### *« Dispositions relatives aux investissements en provenance des États membres de la Communauté européenne*

**Article R. 153-3** – Constitue un investissement au sens de la présente section le fait pour un investisseur :

«1°) soit d'acquérir le contrôle, au sens de l'article L. 233-3 du Code du commerce, d'une entreprise dont le siège social est établi en France ;

«2°) soit d'acquérir directement ou indirectement tout ou partie d'une branche d'activité d'une entreprise dont le siège social est établi en France.

**Article R. 153-4** – Sont soumis à une procédure d'autorisation au sens de l'article L. 151-3, s'ils relèvent de l'article R. 153-3, les investissements réalisés dans les activités énumérées du 8° au 11° de l'article R. 153-2 par une personne physique ressortissante d'un État membre de la Communauté européenne, par une entreprise dont le siège social se situe dans l'un de ces mêmes États ou par une personne physique de nationalité française qui y est résidente.

**Article R. 153-5** – Sont soumis à une procédure d'autorisation au sens de l'article L. 151-3, s'ils relèvent du 2°) de l'article R. 153-3, les investissements réalisés par une personne physique ressortissante d'un État membre de la Communauté européenne, par une entreprise dont le siège social se situe dans l'un de ces mêmes États ou par une personne physique de nationalité française qui y est résidente, dans les activités suivantes :

«1°) activités de casinos, au sens de la loi du 15 juin 1907 modifiée réglementant les jeux dans les casinos des stations balnéaires, thermales et climatiques, dans la mesure où le contrôle de l'investissement est exigé par les nécessités de la lutte contre le blanchissement de capitaux ;

«2°) activités de sécurité privée, au sens de la loi n° 83-629 du 12 juillet 1983 modifiée réglementant les activités privées de sécurité, lorsque les entreprises qui les exercent :

«a) fournissent une prestation à un opérateur public ou privé d'importance vitale, au sens de l'article L. 1332-1 du Code de la défense ;

«b) ou participent directement et spécifiquement à des missions de sécurité définies aux articles L. 282-8 du Code de l'aviation civile et L. 324-5 du Code des ports maritimes ;

«c) ou interviennent dans les zones protégées ou réservées, au sens de l'article 413-7 du Code pénal et des textes pris en application du décret n° 98-608 du 17 juillet 1998 relatif à la protection des secrets de la défense nationale ;

«3°) activités de recherche, de développement ou de production, lorsqu'elles intéressent exclusivement :

«a) les agents pathogènes, les zoonoses, les toxines et leurs éléments génétiques ainsi que leurs produits de traduction mentionnés aux alinéas 1C351 et 1C352a. 2 de l'annexe I du règlement (CE) n° 1334/2000 du Conseil du 22 juin 2000 modifié instituant un régime communautaire de contrôle des exportations de biens et technologies à double usage ;

«b) les moyens de lutte contre les agents prohibés au titre de la convention sur l'interdiction de la mise au point, de la fabrication, du stockage et de l'emploi des armes chimiques et de leur destruction, faite à Paris le 13 janvier 1993, et que le contrôle de l'investissement est exigé par les nécessités de la lutte contre le terrorisme et de la prévention des conséquences sanitaires de celui-ci ;

«4°) activités de recherche, développement, production ou commercialisation portant sur les matériels conçus pour l'interception des correspondances et la détection à distance des conversations définis à l'article 226-3 du Code pénal, dans la mesure où le contrôle de l'investissement est exigé par les nécessités de la lutte contre le terrorisme et la criminalité ;

«5°) activités de services dans le cadre de centres d'évaluation agréés dans les conditions prévues au décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, lorsque les entreprises qui les exercent fournissent ces prestations au profit de services de l'État, dans la mesure où le contrôle de l'investissement est exigé par les nécessités de la lutte contre le terrorisme et la criminalité ;

«6°) activités de production de biens ou de prestations de services dans le secteur de la sécurité des systèmes d'information exercées par une entreprise liée par un contrat passé avec un opérateur public ou privé d'installation d'importance exercées par une entreprise liée par un contrat passé avec un opérateur public ou privé d'installation d'importance vitale au sens des articles L. 1332-1 à L. 1332-7 du Code de la défense pour protéger cette installation ;

«7°) activités relatives aux biens et technologies à double usage énumérées à l'annexe IV du règlement du 22 juin 2000 précité exercées au profit d'entreprises intéressant la défense nationale.»

## Prévention du terrorisme

Le terrorisme pose un problème de définition s'il n'est appréhendé que sous l'angle de l'idéologie. C'est pourquoi il est préférable de s'en tenir à une définition juridique, celle retenue, pour ce motif encore, dans le Livre IV du Code pénal 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 concernant notamment 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 suivantes 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.

Dès lors, 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.

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»).

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.

Cette «*entreprise*», selon la circulaire susvisée 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) ».

À cet égard, 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 symboliques 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 en brisant sa résistance afin de promouvoir une cause ou faciliter le succès d'une revendication.

On voit donc que n'importe quelle action d'expression ou de revendication politique, ou syndicale violente et susceptible de troubler l'ordre public, ne saurait être qualifiée de terroriste.

L'article 3 de la loi du 10 juillet 1991 dispose que les interceptions de sécurité peuvent être consenties pour la « *prévention* du terrorisme ». Les interceptions vont donc se situer en amont du passage à l'acte afin d'en empêcher la commission.

Tout l'enjeu est là : 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 la pensée. 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, l'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) avant que celle-ci ne soit activée pour planifier un ou plusieurs attentats qui, s'ils étaient commis, seraient mis au passif d'autorités publiques imprévoyantes ou angéliques. 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.

On le voit; la frontière est mince mais, s'agissant de certains mouvements tels que ceux énumérés par la dernière décision du Conseil de l'Union européenne en la matière, à savoir celle du 29 mai 2006 (*JOCE* du 31 mai), l'exemple des attentats récents à travers le monde nous enseigne que le basculement peut être rapide et qu'il requiert par conséquent une surveillance très en amont du passage à l'acte.

À ce propos on notera que la préparation en France d'actes à caractère terroriste devant être commis à l'étranger sont susceptibles comme tels de recevoir une qualification pénale (*cf.* article 113-2 alinéa 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 entrent naturellement dans le champ de ce motif légal d'interception.

## Prévention de la criminalité et de la délinquance organisées

Comme les chiffres l'ont encore montré cette année (*cf. supra* p. 17 s.) et en dépit de la permanence 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, 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. Au plan statistique la Commission retient alors la finalité terroriste quand celle-ci est connue.

Cette précision donnée, il n'est pas inutile de s'interroger sur ce concept qui, il y a peu, n'existait pas strictement à l'identique dans le Code pénal. Le Code pénal traitait quant à lui des infractions « commises en bande organisée ». La loi du 9 mars 2004 cependant a consacré dans le Livre IV du Code de procédure pénale un Titre XXV<sup>e</sup> à la « procédure applicable à criminalité et à la délinquance organisée », concernant l'ensemble des infractions aggravées par la circonstance de commission en bande organisée (*cf.* article 706-73 du Code de procédure pénale)<sup>1</sup>. 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 3 de la loi du 10 juillet 1991.

La CNCIS s'était naturellement penchée très tôt sur la définition de ce motif (*cf.* rapports d'activité 1994, p. 18 et 1995, p. 30) et avait souligné que celle-ci résultait tant de celle retenue par la commission Schmelck, que de la définition que donne le Code pénal de la bande organisée à l'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 tel que l'Office central pour la répression du banditisme (OCRB).

---

1) Qui vise également et surtout l'association de malfaiteurs de l'article 450-1 du Code pénal.

La commission entendait par là faciliter la lutte en amont contre la grande criminalité. L'article 132-71 du Code pénal, quant à lui, 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 visait les formes classiques du banditisme (trafic de stupéfiants, proxénétisme, enlèvement rackets, etc.).

Depuis le 1<sup>er</sup> mars 1994, date d'entrée en vigueur du nouveau Code pénal, la liste n'a cessé de s'allonger spécialement avec l'entrée en vigueur de la loi n° 2004-204 du 9 mars 2004 dite Perben II qui a notamment assimilé la direction de groupement ou d'entente à caractère terroriste à une forme de criminalité organisée.

Ainsi la direction d'un groupement ou d'une entente établie en vue de la préparation d'actes terroristes relève désormais au plan pénal de la criminalité organisée. Les interceptions de sécurité ordonnées dans des hypothèses semblables continueront cependant d'être comptabilisées au titre du motif terrorisme.

Sous l'empire de l'ancien Code pénal était réputée « bande organisée tout groupement de malfaiteurs établi en vue de commettre un ou plusieurs vols aggravés [...] et caractérisé par une préparation ainsi que par la possession des moyens matériels utiles à l'action ». C'était là une définition très restrictive quant à son champ d'application, réduit au vol.

Les rédacteurs du nouveau Code pénal ont souhaité faciliter la répression du « crime organisé » protéiforme : « la plus redoutable menace – disait 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, c'est le groupement, la réunion de plusieurs malfaiteurs. Mais 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 organisée du 15 novembre 2000 signée par la France le 12 décembre 2003 dispose que :

- a) 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 ;
- b) 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 ;
- c) 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 (considérant 13 et 14) relative à l'examen de la notion de criminalité organisée dans la loi du 9 mars 2004 (dite Perben II) *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 (cf. article 311-9 du même Code).

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 relèvent pas d'une 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.

En bref on ne saurait, sans dévoyer le motif, de la loi, mettre sur le même plan la suspicion d'approvisionnement du consommateur voire du petit dealer de drogue chez son fournisseur habituel situé de l'autre côté de la frontière et celle d'acheminement depuis un pays lointain d'un container de produits stupéfiants suivi de bout en bout par un cartel même si, dans les deux cas, on peut parler d'un « trafic international de stupéfiants ». Admettre dans le premier cas la commission en bande organisée, avec ses conséquences procédurales et l'aggravation concomitante de la sévérité des peines encourues seraient contraire au principe de proportionnalité.

La Commission entend donc réserver le recours à ce motif légal à des agissements d'une gravité certaine, sous-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.

---

# Interceptions de sécurité et secret-défense

Aux termes de l'article 2 de **l'arrêté du 25 août 2003** relatif à la protection du secret de la défense nationale et portant instruction générale interministérielle sur la protection du secret de la défense nationale, « présentent un caractère de secret de la défense nationale au sens des articles 413-9 et suivants du Code pénal les renseignements, procédés, objets, documents, données informatisées ou fichiers :

- intéressant la défense nationale qui ont fait l'objet de mesures de protection destinées à restreindre leur diffusion ;
- dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale.

Pris en application des dispositions du dernier alinéa de l'article 413-9 du Code pénal, le décret n° 98-608 du 17 juillet 1998 :

- définit trois niveaux de classification : très secret-défense, secret-défense, confidentiel-défense ;
- prévoit que les informations ou supports protégés portent la mention de leur niveau de classification.

La classification « secret-défense » d'un document ou d'une information répond, aux termes de l'article 2 de l'arrêté du 25 août 2003 sus-visé, à deux exigences cumulatives :

- une exigence de fond : l'information ou le document doit intéresser la défense nationale ;
- une exigence de forme : l'apposition de la mention « secret-défense ».

**La notion de défense nationale doit être entendue largement.** Elle trouve sa définition dans l'article 1 de l'ordonnance 59-147 du 7 janvier 1959 portant organisation générale de la défense (ordonnance-cadre) :

« La défense a pour objet d'assurer **en tout temps, en toutes circonstances et contre toutes les formes d'agression**, la sécurité et l'intégrité du territoire, ainsi que la vie de la population. »

Le rapport d'activité 2001-2003 de la Commission nationale consultative du secret de la défense nationale éclaire cette définition en ces termes : « La défense s'exerce, comme le stipule l'ordonnance de 1959 en tous temps et en tous lieux, et concerne tous les secteurs d'activité ; défense militaire du pays, mais aussi défense civile, sécurité intérieure, protection des activités financières, économiques ou industrielles, protection du patrimoine scientifique et culturel de la France ».

Le décret du 17 juillet 1998 réduisant le secret-défense à la notion de défense nationale, contrairement au décret du 12 mai 1981 qui faisait référence, de manière redondante, aux notions de défense nationale et de sûreté de l'État, n'a fait que se conformer à la « définition cadre » issue de l'ordonnance de 1959.

**Au regard de l'article 1 de l'ordonnance du 7 janvier 1959 dont la définition de la défense nationale préfigure la notion d'« intérêts fondamentaux de la nation » de l'article 410-1 du Code pénal** qui recouvre elle-même le domaine de l'article 3 de la loi du 10 juillet 1991, il n'est pas douteux que la classification de tous les éléments relatifs à une interception de sécurité s'impose. Les interceptions de sécurité intéressent la défense nationale et les informations qui y sont relatives sont revêtues de la mention secret-défense.

La position prise dès ses débuts par la CNCIS, éclairée par les travaux parlementaires, d'appliquer à la lettre l'article 17 de la loi du 10 juillet 1991 (quant à la non-information du requérant de l'existence ou la non-existence d'une interception de sécurité *cf.* présent rapport p. 28) est conforme à l'architecture normative concernant le secret de la défense nationale.

Ainsi « 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 » (article 17 loi du 10 juillet 1991).

---

# Jurisprudence européenne et française

## Jurisprudence européenne

L'examen de la jurisprudence de la Cour européenne des droits de l'homme permet, année après année de confirmer l'examen scrupuleux par cette juridiction du délicat équilibre entre le principe du secret des correspondances (quelqu'en soient les supports) proclamé par l'article 8 paragraphe 1 de la Convention européenne des droits de l'homme et le nécessaire aménagement de ce principe à la faveur d'exceptions prévues au paragraphe 2 du même article qui constituent des ingérences étatiques au sein de ce secret protégé.

Il en est ainsi de la décision **Weber et Saravia contre Allemagne – décision n° 54934/00 du 29 juin 2006** où la Cour réaffirme sa volonté d'adosser à sa jurisprudence antérieure (*arrêt Klass* du 6 septembre 1978 en l'occurrence) son examen des critères justifiant une telle atteinte.

La Cour européenne des droits de l'homme a de fait, dégagé deux critères d'examen pour tout dispositif se prévalant du paragraphe 2 de l'article 8 de la Convention :

- un critère *formel* : l'ingérence **publique** dans le secret des correspondances doit être prévue «**par la loi**» qui doit en outre revêtir certaines qualités ;
- un critère *matériel* : celui de la **proportionnalité**. L'atteinte à la vie privée en général et au secret des correspondances de manière plus spécifique, doit constituer « 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 ».

Statuant sur la loi G10 allemande prévoyant le recours à des interceptions de correspondances téléphoniques dans le cadre d'une surveillance stratégique, la Cour a estimé, dans le cadre de son « contrôle formel » que cette loi revêtait les qualités « d'accessibilité » et que les dispositions discutées, au sein de cette loi, envisagées dans leur contexte législatif, renfermaient les garanties minimales contre une ingérence arbitraire telle que définie par la jurisprudence de la Cour et donnaient donc aux citoyens une indication adéquate quant aux circonstances et aux conditions dans lesquelles les autorités publiques étaient autorisées à recourir à des mesures de surveillance, ainsi qu'à l'étendue et aux modalités d'exercice du pouvoir discrétionnaire de ces autorités (critère de *prévisibilité*).

Quant à l'examen du critère « matériel », la Cour indique que les « buts légitimes » poursuivis étaient la sécurité nationale et/ou la prévention du crime.

Quant à la « nécessité, dans une société démocratique », des ingérences, la Cour reconnaît que les autorités nationales jouissent d'une marge d'appréciation relativement ample pour choisir les moyens de protéger la sécurité nationale. Néanmoins, la Cour doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus car un système de surveillance secrète destiné à protéger la sécurité nationale crée un risque de saper, voire de détruire, la démocratie au motif de la défendre.

Quant à la surveillance stratégique en soi, la loi G10 dans sa teneur modifiée avait certes élargi l'éventail des sujets de nature à faire l'objet d'une telle surveillance, mais les garanties contre les abus étaient énoncées de manière exhaustive et la Cour constitutionnelle fédérale les a en fait renforcées pour une infraction au moins. La Cour est convaincue qu'il existait une procédure administrative destinée à empêcher que les mesures fussent prises au hasard, irrégulièrement ou sans étude appropriée. Concernant la supervision et le contrôle des mesures de surveillance, le système était essentiellement le même que celui que la Cour avait jugé ne pas emporter violation de la Convention dans l'*arrêt Klass et autres*; elle ne voit aucune raison de parvenir à une autre conclusion en l'espèce.

Pour ce qui est de la transmission au gouvernement fédéral de données personnelles non anonymes recueillies par le service fédéral des renseignements, la Cour reconnaît que la communication de données personnelles – par opposition à des données anonymes – peut se révéler nécessaire. Les garanties additionnelles introduites par la Cour constitutionnelle fédérale, à savoir que les données personnelles contenues dans le rapport au gouvernement fédéral devaient être signalées et demeurer liées aux buts ayant justifié leur collecte, sont suffisantes pour limiter l'utilisation des informations obtenues à ce qui est nécessaire aux fins de la surveillance stratégique.

## Jurisprudence française

### **Cour de cassation – Chambre criminelle 14 février 2006 – Éléments d’arrêt**

Atteinte à l’intimité de la vie privée – enregistrement téléphonique – absence de consentement des intéressés – contenu strictement professionnel.

Articles 226-1 du Code pénal, 593 du Code de procédure pénal

Moyen du pourvoi

L’arrêt attaqué a renvoyé Mikaël Z... des fins de poursuites du chef d’atteinte à la vie privée par captation de transmission des paroles d’une personne;

Aux motifs qu’il ressort des transcriptions des conversations enregistrées que celles-ci ont porté exclusivement sur les attestations établies par Sébastien Y... et Christian X... pour le procès prud’homal et sur la façon dont elles avaient été rédigées et recueillies; aucun propos touchant à la vie privée des intéressés, c’est-à-dire concernant leurs relations familiales ou amicales, leur vie conjugale ou sentimentale, leur vie physique ou leur état de santé, n’a été retranscrit; dès lors, ces captations de conversations ne portent pas atteinte à la vie privée de ces interlocuteurs même si c’est à leur insu qu’il a enregistré ces conversations; à défaut d’élément intentionnel, le prévenu sera renvoyé des fins de la poursuite;

Alors, d’une part, que caractérise en tous ses éléments le délit d’atteinte à la vie privée par captation des paroles d’une personne, prévu et réprimé par l’article 226-1 du Code pénal, le fait, expressément constaté par la cour d’appel, pour un salarié licencié de téléphoner à ses anciens collègues, auteurs d’attestations produites dans le procès prud’homal, à leur domicile, sur leur ligne téléphonique personnelle, sur le ton de l’amitié, et de leur demander des renseignements sur les circonstances de la rédaction de ces attestations, à titre amical et personnel, en enregistrant sciemment les propos à leur insu;

Alors, d’autre part, que l’arrêt, qui constatait que Mikaël Z... avait enregistré, sans le consentement de ses interlocuteurs, des paroles prononcées à titre privé ou confidentiel, ce qui caractérisait l’élément matériel du délit de l’article 226-1 du Code pénal, ne pouvait exclure tout élément intentionnel en se fondant sur une définition purement abstraite de l’atteinte à l’intimité de la vie privée, sans déduire les conséquences qui s’évinçaient de ses propres constatations relatives au caractère privé et confidentiel des paroles enregistrées à l’insu de ses interlocuteurs, et sans rechercher si Mikaël Z... avait agi ainsi en sachant qu’en enregistrant ces conversations à l’insu de ses interlocuteurs il portait atteinte à l’intimité de leur vie privée, méconnaissant ainsi les textes susvisés;

Alors encore que, comme le faisaient valoir les demandeurs, les conversations enregistrées à leur insu l'ont été en dehors du temps et du lieu de travail, sur des lignes téléphoniques privées, dans un contexte de relations personnelles, sinon amicales, entre les interlocuteurs; qu'ainsi, en tenant compte exclusivement du fait que les propos ont porté sur les attestations rédigées par Christian X... et Sébastien Y... pour le procès prud'homal opposant Mikaël Z... à son employeur, sans replacer ces conversations dans leur contexte, ayant consisté à pénétrer dans la sphère de la vie privée des intéressés pour mieux les déstabiliser, et à se placer dans le cadre de relations purement personnelles pour obtenir d'eux qu'ils se dédisent des attestations fournies à leur employeur commun, en les mettant en confiance par des formules banales : « Ça va?... en forme? », pour mieux leur extorquer, sur un ton badin, des confidences enregistrées à leur insu, la cour d'appel n'a pu justifier légalement sa décision »;

#### Motifs de l'arrêt

Attendu qu'il résulte de l'arrêt attaqué et des pièces de procédure que Mikaël Z... a, au cours de l'instance prud'homale l'opposant à la société Socaelec et relative à son licenciement, versé aux débats la transcription, par huissier, de deux conversations téléphoniques enregistrées par ses soins, intervenues entre lui et ses anciens collègues de travail, Sébastien Y... et Christian X..., avec lesquels il avait pris contact à la suite de la production, par la société Socaelec, d'attestations émanant de ceux-ci; que la société Socaelec, Sébastien Y... et Christian X... l'ont cité devant le tribunal correctionnel, du chef d'atteinte à l'intimité de la vie privée;

Attendu que, pour renvoyer le prévenu des fins de la poursuite, l'arrêt énonce que les conversations, bien qu'enregistrées par Mikaël Z... à l'insu de ses interlocuteurs, ont porté exclusivement sur les conditions de rédaction des attestations produites par la société Socaelec lors de l'instance prud'homale et qu'aucune information ne touchait à la vie privée des intéressés;

Attendu qu'en l'état de ces énonciations, d'où il résulte que ces propos entraient dans le cadre de la seule activité professionnelle des intéressés et n'étaient pas de nature à porter atteinte à l'intimité de leur vie privée, les juges ont justifié leur décision;

D'où il suit que le moyen doit être écarté;

Et attendu que l'arrêt est régulier en la forme;

[...]

Rejette le pourvoi.

## **Cour de cassation – Chambre criminelle 1<sup>er</sup> mars 2006 – Éléments d’arrêt**

Criminalité organisée – sonorisations et fixations d’images de certains lieux ou véhicules – sonorisation du parloir d’un détenu – régularité – atteinte au principe de la loyauté des preuves.

Articles 6-1 et 8 de la Convention européenne des droits de l’homme, 591, 593, 706-960, 706-102 du Code de procédure pénale;

Moyen du pourvoi

L’arrêt attaqué a refusé de prononcer la nullité des actes de la procédure tirée de l’irrégularité de la sonorisation du parloir de Catherine Y...;

Aux motifs que, « par commission rogatoire du 12 mai 2005, les magistrats instructeurs ordonnaient la mise en place d’un dispositif de sonorisation des parloirs de Catherine Y... avec les personnes habilitées à lui rendre visite; ce procédé avait déjà été utilisé lors des premiers mois de détention provisoire de Georges Z...; que les conseils de Michel X... considèrent qu’il s’agit à la fois d’une atteinte à la vie privée, d’une provocation de juges visant à se procurer des éléments de preuve contre leur client et donc d’une atteinte aux droits de la défense; que les trois procès-verbaux ont été établis, qui ne font apparaître dans la retranscription des conversations tenues aucun élément déterminant ou nouveau à l’encontre des personnes mises en examen ou en cause;

Que Catherine Y... a été mise supplétivement en examen le 13 avril 2005 pour recel de blanchiment de produits d’un trafic de stupéfiants, recel de blanchiment aggravé, il était donc possible aux magistrats instructeurs de faire application des dispositions de l’article 706-96 du Code de procédure pénale, lesquelles renvoient à celles de l’article 706-73, 4 du même Code, s’agissant de faits de recel; que cette disposition de la loi du 9 mars 2004, qui précise que la mise en place du dispositif technique se fait sans le consentement des intéressés en des lieux publics ou privés déterminés par le juge d’instruction et permet l’enregistrement de paroles prononcées par une ou plusieurs personnes à titre privé ou confidentiel, a fait l’objet, avant d’être votée et promulguée, – après avis du Conseil constitutionnel –, de débats qui ont démontré la volonté du législateur de choisir entre l’éventuelle atteinte à la vie privée et la nécessaire adaptation des moyens policiers et judiciaires d’investigations pour contrer la délinquance organisée;

Qu’en conséquence, la mise en place d’un dispositif d’écoutes et la transcription des paroles entendues ne peuvent porter atteinte aux droits de la défense, puisque réalisées conformément à une disposition législative et sous le contrôle d’un juge;

D’autant que la retranscription de ces écoutes, ainsi qu’il ressort du contenu des procès-verbaux contestés, ne comporte que les propos relatifs à la procédure en cours et ne fait nullement état de faits concernant la

vie privée et l'intimité des intéressés ; qu'issue de la loi du 9 mars 2004, organisée sous le contrôle du juge, dans le cadre des articles 706-96 à 706-102 du Code susvisé, la décision de recourir à ce procédé ne peut constituer une fraude aux droits de la défense, ni constituer un moyen déloyal d'obtention de preuve, alors qu'elle résulte de l'utilisation régulière d'un dispositif légal d'investigations, mis à la disposition du juge, que les procès-verbaux de transcription figurent en procédure et peuvent être critiqués par les conseils des mis en examen, et qu'il ne peut être raisonnablement avancé, sans suspecter l'impartialité des juges et porter atteinte à leur honneur ;

Que les magistrats instructeurs, en autorisant Catherine Y... à rencontrer des membres de sa famille et ses amies, dont plusieurs avaient déjà été entendues comme témoins ou le seraient postérieurement à la date de la commission rogatoire, n'ont visé qu'à obtenir de nouveaux éléments à charge contre Michel X... ; que, sur cet argument spécifique, outre la nécessité de vérifier l'adéquation des déclarations de Catherine Y... faites le 11 mai 2005 et des propos qu'elle pourrait tenir avec sa famille, la mesure d'investigation ordonnée le 12 mai 2005 doit aussi s'analyser comme une recherche de la vérité, s'inscrivant dans le cadre des dispositions générales de l'article préliminaire du Code de procédure pénale – dont il est constant qu'il n'est pas contraire à l'article 6 de la Convention européenne des droits de l'homme – et commandée par une réserve certaine à l'égard des révélations faites par Catherine Y... à l'encontre de l'avocat de Georges Z..., et ce, préalablement à son éventuelle interpellation ; qu'enfin, la mise en œuvre de ce dispositif s'inscrit dans les autres actes d'enquête effectués par les magistrats instructeurs et notamment le recueil de déclarations de Gilles S... et d'autres mis en examen, venant conforter les déclarations de Catherine Y... » ;

Alors que, d'une part, les « mesures de sauvegarde », prévues par les dispositions des articles 706-96 à 706-102 du Code de procédure pénale issus de la loi du 9 mars 2004, ne sont pas suffisantes pour justifier que l'ingérence dans la vie privée du détenu et de ses proches que constitue la sonorisation d'un parloir est désormais « prévue par la loi » ;

Alors qu'en tout état de cause, les dispositions qui encadrent la procédure de sonorisation ne permettent pas pour autant l'exercice d'un « contrôle efficace » pour un justiciable qui, comme en l'espèce, du fait d'une écoute incidente se voit mis en cause dans une procédure à laquelle il était étranger ;

Alors qu'en outre, il résulte des mentions mêmes de la chambre de l'instruction que la sonorisation du parloir de Catherine Y... avait pour objet de « vérifier l'adéquation des déclarations faites par celle-ci lors d'un interrogatoire et des propos qu'elle pouvait tenir avec sa famille », sachant que cette mesure d'investigation devait aussi s'analyser comme « une recherche de la vérité » ; qu'en l'état de ces seuls motifs, la chambre de l'instruction n'a pas caractérisé que l'ingérence dans la vie privée de

Catherine Y... et de ses proches était « nécessaire » pour atteindre l'un des buts « légitimes » prévus par l'alinéa 2 de l'article 8 de la Convention européenne des droits de l'homme ;

Alors qu'enfin, la sonorisation d'un parloir qui aboutit en pratique à ce que le juge d'instruction puisse enregistrer à leur insu des personnes qu'il a d'ores et déjà entendues en qualité de témoin et auxquelles il a, en toute connaissance de cause, délivré un permis de visite, constitue un détournement de procédure et un procédé déloyal de d'obtention de la preuve pénale » ;

#### Motifs de l'arrêt

Attendu qu'en écartant, par les motifs reproduits au moyen, le grief pris d'une violation de l'article 8 de la Convention européenne des droits de l'homme, la chambre de l'instruction a justifié sa décision ;

Que, d'une part, l'interception des conversations de Catherine Y... et de ses visiteurs au parloir de la maison d'arrêt a eu lieu dans les conditions et formes prévues par les articles 706-96 à 706-102 du Code de procédure pénale ;

Que, d'autre part, les opérations, ordonnées par le juge d'instruction, pour une durée limitée, ont été placées en permanence sous son autorité et son contrôle et ont été justifiées par la nécessité de rechercher la manifestation de la vérité, relativement à des infractions portant gravement atteinte à l'ordre public, telles celles prévues et définies par l'article 706-73, alinéa 14, du Code de procédure pénale ;

Qu'enfin, la Cour de cassation est en mesure de s'assurer que les garanties légales et conventionnelles reconnues aux personnes concernées par cette mesure ont été respectées, celles-ci ayant tout pouvoir d'en contrôler efficacement l'exécution ;

Sur le moyen, pris en ses deuxième et quatrième branches :

Attendu que, pour écarter le moyen de nullité, proposé par Michel X..., pris de l'emploi d'un procédé déloyal d'obtention de la preuve d'une infraction et d'une atteinte aux droits de la défense, l'arrêt attaqué relève que le juge d'instruction, aux fins de rechercher la manifestation de la vérité, a eu recours à un dispositif de sonorisation prévu par la loi ; que les juges ajoutent qu'en l'espèce la sonorisation du parloir de Catherine Y... était commandée par la réserve qu'appelaient les accusations qu'elle avait portées contre Michel X... à l'occasion d'un interrogatoire ; qu'enfin, la chambre de l'instruction retient que l'intéressé a été en mesure d'exercer son droit à contester le contenu des procès-verbaux de transcription des conversations enregistrées, régulièrement versés dans la procédure ;

Attendu qu'en statuant ainsi, la chambre de l'instruction a justifié sa décision ;

D'où il suit que le moyen doit être écarté ;  
Et attendu que l'arrêt est régulier en la forme ;  
[...]  
Rejette le pourvoi.

### **Cour de cassation – Chambre criminelle 18 janvier 2006 – Éléments d'arrêt**

Écoutes téléphoniques – conversation entre l'avocat et un proche de son client – confidentialité – validité

Article 6 et 8 de la Convention européenne des droits de l'homme

Article 432-4 du Code pénal 100-5, 100-7, 171, 206, 591, 593 et 802 du Code de procédure pénale

Moyen du pourvoi

L'arrêt attaqué a rejeté la demande d'annulation des interceptions et transcriptions des conversations téléphoniques passées sur la ligne de l'avocat de Sony et Vito X... (cotes D 2946 à D 2949), de la cote D 3002 s'y référant expressément ainsi que la procédure subséquente ;

Aux motifs que celui qui invoque une irrégularité d'une formalité protectrice du droit des parties n'a qualité à le faire que si cette irrégularité le concerne ; que Sony X... et Vito X... sont sans qualité pour contester la régularité de l'interception et de la transcription, ordonnées par commission rogatoire du juge d'instruction, de conversations échangées, sur une ligne téléphonique qui ne leur est pas attribuée, entre une tierce personne, en l'espèce leur père, et son avocat, qui se trouve être aussi le leur ; que, par ailleurs, la chambre de l'instruction n'a pas à répondre à leur demande de relever d'office d'autres moyens de nullité de la procédure ;

Alors que la règle procédurale selon laquelle un mis en examen est sans qualité pour contester la régularité de l'interception et de la transcription ordonnées par commission rogatoire du juge d'instruction de conversations échangées entre d'autres personnes sur une ligne qui ne lui est pas attribuée, reçoit exception, conformément au principe fondamental de la loyauté des preuves, du principe d'une libre défense et du caractère strict du secret professionnel, lorsque les interceptions et les retranscriptions dont s'agit, opérées en méconnaissance des formalités substantielles de l'article 100-7 du Code de procédure pénale, ont eu pour but et pour effet d'opposer à ce mis en examen les propos de son propre avocat en dehors de toute participation alléguée de ce dernier à une activité délictueuse ;

Alors que le secret professionnel de l'avocat, élément essentiel du procès équitable, s'étend nécessairement, au-delà des propos échangés

entre lui et son client aux propos échangés entre cet auxiliaire de justice et les proches de ce client et que, par conséquent, le mis en examen établit l'existence d'un grief personnel dès lors que lui est opposée dans la procédure la retranscription de conversations téléphoniques entre son propre avocat et son propre père ;

Alors que, même si elle a été surprise à l'occasion d'une mesure d'instruction régulière, la conversation entre un avocat et son client ou entre un avocat et un proche de son client ne peut être retranscrite et versée au dossier de la procédure sans que cette mesure soit considérée comme attentatoire aux libertés individuelles au sens de l'article 432-4 du Code pénal ;

Alors qu'il appartient, en tout état de cause, à la chambre de l'instruction de prononcer, au besoin d'office, l'annulation des interceptions et retranscriptions d'écoutes téléphoniques portant atteinte au principe fondamental du secret professionnel de l'avocat garanti par les principes déduits des articles 6 et 8 de la Convention européenne des droits de l'homme et des libertés fondamentales et les textes susvisés » ;

#### Motifs de l'arrêt

Attendu qu'il résulte de ces textes que, même si elle est surprise à l'occasion d'une mesure d'instruction régulière, la conversation entre un avocat et l'un de ses clients ne peut être transcrite et versée au dossier de la procédure que s'il apparaît que son contenu est de nature à faire présumer la participation de cet avocat à une infraction ; que la violation de ce principe doit être relevée, même d'office, par la chambre de l'instruction chargée d'examiner, en application de l'article 206 du Code de procédure pénale, la régularité de la procédure qui lui est soumise ;

Attendu que, pour rejeter le moyen d'annulation proposé par Sony et Vito X..., pris de l'irrégularité de l'enregistrement et de la transcription dans le dossier de la procédure de conversations téléphoniques échangées entre leur père et son avocat, qui, aux termes de l'arrêt attaqué ; « se trouve être aussi le leur », les juges relèvent que les requérants sont sans qualité pour contester l'interception et la transcription, ordonnées sur commission rogatoire du juge d'instruction, des conversations échangées, sur une ligne téléphonique qui ne leur est pas attribuée, entre une tierce personne et son avocat ;

Mais attendu qu'en statuant ainsi, sans rechercher, comme elle y était tenue, s'il avait été porté atteinte au principe de la confidentialité des conversations téléphoniques entre un avocat et un client, la chambre de l'instruction a méconnu le sens et la portée des textes susvisés et du principe énoncé ci-dessus ;

D'où il suit que la cassation est encourue ;

Par ces motifs, casse et annule [...]

## **Cour de cassation – Chambre criminelle 23 mai 2006 – Éléments d’arrêt**

Officier de police judiciaire – pouvoirs – réquisitions aux fins d’obtenir la remise de documents – conditions – autorisation du procureur de la République – Forme.

Article 6, 8 et 13 de la Convention européenne des droits de l’homme, 60, 77-1, 100 et suivants, 170, 206, 591 et 593 du Code de procédure pénale.

### Moyen du pourvoi

La chambre de l’instruction a validé les écoutes téléphoniques incriminées et a rejeté en conséquence la requête en annulation de la procédure à compter de la côte D 24;

Aux motifs que, selon l’article 100-3 du Code de procédure pénale, 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; que parmi les conditions d’application de ce texte définies par le décret n° 93119 du 28 janvier 1993 figure l’établissement d’un écrit indiquant tous les éléments d’identification de la liaison à intercepter, la désignation de l’exploitant lui-même comme responsable s’il s’agit d’un réseau non public autorisé et l’obligation pour lui de désigner un agent techniquement compétent dont le casier judiciaire doit être vierge de toute condamnation pénale; qu’il peut être vérifié que les documents adressés aux divers exploitants de réseaux par les services de police sont en tous points conformes aux prescriptions des articles 100 à 100-5 du Code de procédure pénale; que, s’il peut être procédé à l’identification des numéros de téléphone à la demande d’un officier de police judiciaire, cette mesure qui ne vise pas à une constatation ou à un examen technique ou scientifique au sens des articles 60 et 77-1 du Code de procédure pénale, ne rend pas nécessaire une prestation de serment de l’opérateur concerné;

Que les opérations d’interception et de transcription que seul le juge d’instruction peut décider en déléguant leur exécution à un officier de police judiciaire ne constituent pas davantage des opérations à caractère technique; que leur exécution ne nécessite donc pas de la part du représentant de l’exploitant du réseau, légalement habilité, une prestation de serment que le législateur lui-même animé en la circonstance d’un large souci de minutie n’a pas prévu; que la Cour étant ainsi à même de pouvoir s’assurer de la régularité des interceptions critiquées, il conviendra de rejeter le moyen proposé qui n’apparaît pas fondé;

Alors que, d’une part, l’ingérence dans la vie privée des citoyens réalisée par la mise en place d’un dispositif d’écoutes téléphoniques,

quand elle a été requise par l'autorité judiciaire, ne peut être matériellement exécutée par un personnel qui serait lui-même soustrait au contrôle direct de l'autorité mandante; qu'en se refusant en principe à exercer le moindre contrôle de légalité des conditions de réalisation des écoutes incriminées, la chambre de l'instruction a méconnu son office;

Alors que, d'autre part, les opérations tendant à la mise en œuvre technique d'une écoute téléphonique ne peuvent être effectuées que par des personnes qualifiées au sens des articles 60 et 77-1 du Code de procédure pénale; qu'en application de ces textes, ces personnes doivent prêter serment d'apporter leur concours à la justice en leur honneur et conscience;

Alors que, en tout état de cause, la réquisition délivrée à un opérateur privé pour la mise en place d'un dispositif d'écoutes téléphoniques ne peut être réalisée que par des agents spécialement habilités à cette fin; qu'en se bornant à dire que les documents adressés aux opérateurs par les officiers de police judiciaire étaient conformes aux prescriptions des articles 100 à 100-5 du Code de procédure pénale, sans vérifier ni que les responsables intimés figuraient bien sur la liste qu'il appartient au ministre de dresser ni que les agents d'exécution aient eux-mêmes également figuré sur la liste devant être adressée au procureur de la République aux fins de contrôle des exigences prévues par l'article 1<sup>er</sup> du décret n° 93119 du 28 janvier 1993, la chambre de l'instruction a derechef violé les textes et principes visés au moyen »;

Motifs [Attendu que Francis X... et Florent Y..., mis en examen des chefs d'infractions à la législation sur les stupéfiants, ont saisi la chambre de l'instruction, d'une requête excipant de la nullité des réquisitions adressées par l'officier de police judiciaire aux différents exploitants de réseaux de télécommunications, en exécution de commissions rogatoires prescrivant l'interception de communications téléphoniques, au motif qu'en violation des dispositions de l'article 60 du Code de procédure pénale, les représentants de ces opérateurs qui avaient exécuté ces réquisitions, n'avaient pas prêté, par écrit, le serment exigé par ce texte; qu'ils ont soutenu, dans leur mémoire déposé devant la chambre de l'instruction, que les services de télécommunications requis avaient procédé, non seulement à des opérations techniques d'interception mais également « à de véritables constatations techniques par l'analyse et le tri qu'ils ont opérés dans les correspondances pour ne retenir que ce qui est nécessaire à l'accusation »;

Attendu que, pour refuser de faire droit à la demande d'annulation, l'arrêt attaqué énonce que les opérations d'interception et de transcription que seul le juge d'instruction peut décider, ne constituent pas des opérations à caractère technique, et que leur exécution ne nécessite donc pas de la part du représentant de l'exploitant du réseau, légalement habilité, une prestation de serment que le législateur lui-même n'a pas prévue;

Attendu qu'en prononçant ainsi, la chambre de l'instruction a justifié sa décision sans méconnaître les dispositions conventionnelles invoquées;

Que, d'une part, ni l'article 100-3 ni aucune autre disposition du Code de procédure pénale n'exigent que l'agent qualifié requis par l'officier de police judiciaire pour procéder à des interceptions de communications téléphoniques prête serment;

Que, d'autre part, les dispositions de l'article 60 de ce Code, qui ont pour seul objet de régir les réquisitions adressées par l'officier de police judiciaire, au cours de l'enquête de flagrance, à une personne qualifiée pour qu'elle procède à des examens techniques ou scientifiques, sont étrangères aux interceptions de communications téléphoniques ordonnées par le juge d'instruction;

D'où il suit que le moyen qui, en ses première et troisième branches, est nouveau, ne saurait être admis;

Et attendu que l'arrêt est régulier en la forme;

[...] rejette le pourvoi.

---

# Questions parlementaires

## Sécurité publique Fonctionnement – services de renseignements officiels

**98184 -27 juin 2006, Assemblée nationale** – M. Pierre Morel-A-L'Huissier attire l'attention de M. le ministre d'État, ministre de l'Intérieur et de l'Aménagement du territoire, sur les relations qu'entretiennent les différents services de renseignement officiels entre eux. Parmi ces services, trois sont issus de l'armée (DGSE, DRM, DPSD), et deux de la police (DST et RG). Il souhaiterait savoir si ces services peuvent néanmoins mettre en commun leurs informations lorsqu'ils travaillent sur des problématiques similaires.

**Réponse** – Créée en 1944 pour « lutter contre les activités d'espionnage et contre l'ingérence des puissances étrangères sur les territoires relevant de la souveraineté française », la direction de la surveillance du territoire (DST) a vu évoluer de façon importante ses missions pour prendre en compte l'apparition, puis la diversification de la menace terroriste (prolifération des armes nucléaires, bactériologiques, chimiques, balistiques) ainsi que la problématique de la sécurité économique. Ces attributions ont été formalisées par le décret n° 82-1100 du 22 décembre 1982, qui précise que cette direction active de la police nationale est chargée de « lutter contre les activités inspirées, engagées ou soutenues par des puissances étrangères et de nature à nuire à la sécurité ou aux intérêts fondamentaux du pays ».

Conformément au décret n° 95-44 du 16 janvier 1995, la direction centrale des renseignements généraux (DCRG) participe à la défense

des intérêts fondamentaux de l'État et concourt à la mission générale de sécurité intérieure. À ces titres, elle est chargée de « la recherche et de la centralisation des renseignements nécessaires à la prévention et à la lutte contre le terrorisme ainsi que de la surveillance des groupes à risque agissant sur le territoire national » (article 2 de l'arrêté du 6 novembre 1995 relatif à l'organisation et aux missions de la DCRG et de ses services déconcentrés).

La transformation de la 6<sup>e</sup> division de la police judiciaire en division nationale antiterroriste, puis en sous-direction antiterroriste de la direction centrale de la police judiciaire (DCPJ), chargée de la lutte contre le terrorisme national et international, y compris dans ses aspects financiers (arrêté du 19 mai 2006 relatif aux missions et à l'organisation en sous-directions de la direction centrale de la police judiciaire), reflète également l'adaptation des structures de prévention et de lutte contre le terrorisme à l'évolution des menaces.

Toutefois, pour tenir compte de l'évolution des risques terroristes, continuer d'adapter au mieux les moyens d'anticipation et de lutte et développer une véritable stratégie de riposte face à cette menace protéiforme, un Livre blanc sur la sécurité intérieure face au terrorisme a été remis au Gouvernement en mars de cette année. De ses travaux, il en est ressorti notamment que l'action des différents services spécialisés dans la lutte contre le terrorisme nécessite une étroite coordination compte tenu du niveau actuel de la menace.

Cette mission d'ores et déjà assurée, pour les services de police, par l'Unité de coordination de lutte antiterroriste (UCLAT), sera renforcée grâce au travail en synergie des services concernés. Celle-ci sera facilitée par la création d'un pôle de renseignement sur un site unique qui regroupera la direction de la surveillance du territoire, la direction centrale des renseignements généraux et la sous-direction de la lutte antiterroriste de la direction centrale de la police judiciaire. En effet, la complémentarité opérationnelle de ces services sera ainsi mieux à même de s'exprimer, ce qui accroîtra l'efficacité de leur travail pour agir au plus près de la menace et assurer aux citoyens la sécurité et la sûreté qu'ils attendent. La lutte contre le terrorisme est une priorité nationale qui implique que l'ensemble des services concernés, qu'ils relèvent du ministère de l'Intérieur ou du ministère de la Défense, coopèrent. Le comité interministériel du renseignement (structure qui relève du secrétaire général de la Défense nationale) illustre cette orientation grâce aux échanges quotidiens d'informations qu'il permet.

## Ordre public Terrorisme – lutte et prévention – droits de l’homme et libertés publiques – respect

**80467 -13 décembre 2005, Assemblée nationale** – Alors que les menaces terroristes pèsent sur notre pays, l’intérêt national commande de mieux assurer le droit à la sûreté dans le respect des libertés individuelles. Dans ce contexte, M. Dino Ciniéri demande à M. le ministre d’État, ministre de l’Intérieur et de l’Aménagement du territoire, de lui faire part des initiatives qu’il compte prendre afin de répondre à ces menaces dans le respect du nécessaire équilibre entre les exigences de la sécurité et la préservation des libertés de chaque citoyen.

**Réponse** – Pour assurer le droit à la sûreté des citoyens et dans le cadre d’une lutte proactive contre les réseaux terroristes, le ministre d’État, ministre de l’Intérieur et de l’Aménagement du territoire, a souhaité parfaire le dispositif législatif existant. La loi adoptée le 22 décembre 2005 relative à la lutte contre le terrorisme renforce ainsi les moyens des services spécialement habilités pour détecter et neutraliser le plus en amont possible les réseaux terroristes. Les mesures votées répondent aux évolutions de la menace qui pèse sur la France et aux procédés mis en œuvre par les organisations terroristes pour porter atteinte aux institutions. Le recours aux dispositifs juridiques autorisés par le législateur a été strictement encadré afin de garantir le respect des libertés individuelles, en particulier la liberté d’aller et venir.

Ainsi, en matière de vidéosurveillance, seuls les agents de la police et de la gendarmerie nationales, individuellement désignés et habilités, pourront être rendus destinataires des images et des enregistrements sur décision préfectorale après avis de la commission départementale. En cas d’urgence, l’avis est recueilli lors de la prochaine réunion de la commission.

Dans le domaine de l’accès aux données de connexion électroniques, là aussi, seuls les agents individuellement désignés et habilités des services de la police et de la gendarmerie nationales spécialement chargés de lutter contre le terrorisme seront habilités à en connaître. Les demandes d’accès, motivées, seront soumises à la décision d’une personne qualifiée désignée par la Commission nationale de contrôle des interceptions.

Par ailleurs, ce n’est qu’en cas d’imminence d’une action terroriste que le juge des libertés pourra, à titre exceptionnel, décider que la garde à vue en cours d’une personne mise en cause pour crimes et délits constituant des actes de terrorisme, fera l’objet d’une prolongation supplémentaire de 24 heures renouvelable une fois.

## Préoccupations des avocats relatives au respect des droits de la défense

**19629 - 6 octobre 2005, Sénat** – M. Jacques Baudot attire l'attention de M. le garde des Sceaux, ministre de la Justice, sur les préoccupations exprimées par les avocats relatives au respect des droits de la défense et des libertés publiques. Leurs revendications portent, d'une part, sur les écoutes téléphoniques. Ils estiment qu'il faut assurer l'effectivité de l'information du bâtonnier lorsqu'un avocat est écouté, et régler les modalités pour éviter que de fait tous les avocats d'un même cabinet ne soient écoutés puisqu'ils utilisent la même ligne téléphonique.

Par ailleurs, il conviendrait de légiférer pour revenir sur la jurisprudence de la Cour de cassation qui permet la retranscription des conversations du client avec son avocat. D'autre part, la profession s'interroge sur les moyens en personnel et en fonds affectés qui sont prévus pour la mise en œuvre effective des réformes en matière de justice. En conséquence, il lui demande quelles dispositions il entend prendre pour répondre aux inquiétudes des avocats qui souhaitent défendre les justiciables et les citoyens dans le respect des principes fondamentaux qui régissent leur profession : la confidentialité, l'indépendance, la liberté de communication et le secret professionnel.

**Réponse** – Le garde des Sceaux, ministre de la Justice, souhaite assurer l'honorable parlementaire qu'il partage ses préoccupations tendant au respect des droits de la défense dans le cadre du procès pénal. En ce qui concerne les écoutes téléphoniques, il souhaite appeler son attention sur les dispositions de l'article 100-7 du Code de procédure pénale aux termes desquelles « 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 ». En outre, il convient de souligner que la loi n° 2005-1549 du 12 décembre 2005 relative au traitement de la récidive des infractions pénales a introduit un nouvel alinéa dans l'article 100-5 du Code de procédure pénale qui prévoit « [qu'] à peine de nullité, ne peuvent être transcrites les correspondances avec un avocat relevant de l'exercice des droits de la défense ». Par cette modification législative, le législateur a souhaité entériner la jurisprudence de la chambre criminelle de la Cour de cassation aux termes de laquelle « le pouvoir du juge d'instruction de prescrire l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications trouve sa limite dans le respect des droits de la défense qui commande notamment la confidentialité des correspondances téléphoniques de l'avocat désigné par la personne mise en examen » (Crim. 15 janvier 1997 ; Bull. crim. n° 14).

Le garde des Sceaux souhaite faire valoir que l'état du droit positif en matière d'écoutes téléphoniques est le résultat d'un équilibre satisfaisant entre le respect dû aux droits de la défense et la nécessité de

mener certains types d'investigations pour parvenir à la manifestation de la vérité. En ce qui concerne l'interrogation des avocats sur l'existence de moyens suffisants pour permettre la mise en œuvre des réformes en matière de justice, le garde des Sceaux tient à assurer l'honorable parlementaire qu'il partage cette préoccupation légitime et souhaite lui faire part de sa détermination à obtenir, dans le cadre fixé par le Premier ministre, compte tenu des contraintes budgétaires générales, une adaptation des moyens de l'institution judiciaire aux évolutions à venir.

# Table des matières

<b>Avant-propos</b> .....	5
 Première partie	
<b>RAPPORT D'ACTIVITÉ</b> .....	7
Chapitre I	
<b>Organisation et fonctionnement de la Commission</b> .....	9
Composition de la Commission .....	9
Rappel des compositions successives de la Commission .....	10
Missions et Fonctionnement .....	10
Financement.....	11
Chapitre II	
<b>Le contrôle des autorisations</b> .....	13
Le contrôle en amont .....	13
Le contrôle en aval .....	17
Tableaux annexes .....	19
Chapitre III	
<b>Le contrôle de l'exécution</b> .....	25
Enregistrement, transcription et destruction .....	25
Le contrôle du GIC .....	26

Les visites sur le terrain .....	26
Réclamations de particuliers et dénonciation à l'autorité judiciaire .....	27

Chapitre IV

<b>Le contrôle du matériel</b> .....	31
--------------------------------------	----

Chapitre V

<b>Actualités de l'année 2006</b> .....	41
---	----

Le renforcement de la lutte contre le terrorisme : la loi n° 2006-64 du 23 janvier 2006 .....	41
--	----

Deuxième partie

<b>ÉTUDES ET DOCUMENTS</b> .....	43
----------------------------------	----

Chapitre I

<b>Présentation ordonnée des textes relatifs aux interceptions</b> .....	45
--	----

Loi n° 91-646 du 10 juillet 1991 (consolidée) .....	46
---	----

Textes réglementaires récents visant la loi du 10 juillet 1991 .....	56
--	----

Chapitre II

<b>Actualité législative</b> .....	59
------------------------------------	----

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 .....	59
--	----

Décret n° 2006-1405 du 17 novembre 2006 relatif à l'organisation du ministère de la Justice et instituant une délégation aux interceptions judiciaires .....	62
--	----

Chapitre III

<b>Observations sur les motifs légaux d'interception</b> .....	63
--	----

Sécurité nationale .....	63
--------------------------	----

Sauvegarde du potentiel scientifique et économique de la Nation .....	66
---	----

Prévention du terrorisme .....	71
--------------------------------	----

Prévention de la criminalité et de la délinquance organisées .....	73
--	----

Chapitre IV

<b>Interceptions de sécurité et secret-défense</b> .....	77
--	----

Chapitre V	
<b>Jurisprudence européenne et française</b> .....	79
Jurisprudence européenne.....	79
Jurisprudence française.....	81
Chapitre VI	
<b>Questions parlementaires</b> .....	91
Sécurité publique Fonctionnement – services de renseignements officiels.....	91
Ordre public Terrorisme – lutte et prévention – droits de l’homme et libertés publiques – respect.....	93
Préoccupations des avocats relatives au respect des droits de la défense.....	94