



# Commission nationale de contrôle des interceptions de sécurité

**17<sup>e</sup> rapport d'activité**

**Année 2008**

---



# 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 interceptions de sécurité (loi n° 91-646 du 10 juillet 1991)</b> .....	13
Chapitre III	
<b>Le contrôle des opérations de communication des données techniques (loi n° 2006-64 du 23 janvier 2006)</b> .....	29
Deuxième partie	
<b>JURISPRUDENCE DE LA COMMISSION</b> .....	35
Troisième partie	
<b>ÉTUDES ET DOCUMENTS</b> .....	51
Chapitre I	
<b>Présentation ordonnée des textes relatifs aux missions de la Commission</b> .....	53
Chapitre II	
<b>Actualité législative et réglementaire</b> .....	81

Chapitre III	
<b>Interceptions de sécurité et secret-défense .....</b>	<b>85</b>
Chapitre IV	
<b>Jurisprudence des cours et tribunaux .....</b>	<b>87</b>

# Avant-propos

L'année 2008 se situe, pour la Commission, dans la droite ligne des évolutions amorcées en 2006 et 2007.

Certes, le paysage politique et administratif dans lequel s'insère notre activité de contrôle fondée sur les lois de 1991 et de 2006 a-t-il changé.

Au niveau politique, le Conseil national du renseignement a été mis en place auprès du Président de la République, suite aux préconisations du Livre blanc sur la défense et la sécurité intérieure; le nouveau « coordonnateur national du renseignement » a notamment pour mission d'assurer la préparation et de veiller à l'exécution des décisions du Conseil.

Le Parlement a, de son côté, mis en place la « délégation parlementaire au renseignement » créée par la loi du 9 octobre 2007.

Au niveau administratif, une importante réforme a vu le jour avec la création de la nouvelle Direction centrale du renseignement intérieur (DCRI) qui regroupe les missions dévolues à la DCRG et à la DST.

La Commission de contrôle, pour ce qui la concerne, a poursuivi sa tâche dans ce nouveau cadre, et avec ce nouvel acteur qu'est la DCRI.

Les chiffres n'ont guère changé : un peu moins de 6000 interceptions de sécurité (demandes initiales et renouvellements) pour lesquelles est recueilli l'avis *a priori* de la Commission et environ 38000 décisions de la « personnalité qualifiée » concernant les données techniques de connexion soumises au contrôle *a posteriori* de la Commission.

S'agissant des interceptions de sécurité, ces chiffres devraient, dans un premier temps, légèrement reculer en 2009, compte tenu de la nouvelle jurisprudence de la Commission qui permet de ne plus compter les « urgences techniques ».

Cet allègement très partiel, sur le plan des tâches de pure gestion administrative, permettra en 2009 à la Commission de se concentrer à effectifs constants sur son « cœur de métier », à savoir le contrôle de la motivation des interceptions de sécurité, comme des demandes de données techniques de connexion.

Dans le premier cas, il s'agit de s'assurer, non seulement lors de l'autorisation, mais aussi dans le temps, de l'adéquation de l'écoute au motif invoqué; dans le second, il s'agit de veiller à ce que l'instrument mis en place par la loi de 2006, et dont l'application a été prorogée par la loi du 1<sup>er</sup> décembre 2008, soit effectivement utilisé pour la seule lutte contre la menace terroriste, et non à d'autres fins.

Les méthodes de contrôle de la Commission, qui s'étaient déjà enrichies depuis 2005 avec le contrôle « continu » des productions, se sont encore raffinées en 2008 ainsi que le fait ressortir le chapitre du rapport consacré au contrôle.

Par voie jurisprudentielle, la Commission a continué à raccourcir au cas par cas la durée légale maximale de quatre mois pour laquelle une interception de sécurité peut être demandée. Bien entendu, ceci ne préjuge en aucun cas la possibilité pour les services de solliciter un renouvellement, en produisant les justifications adéquates.

Le contrôle *a posteriori* de l'adéquation du motif invoqué lors de la décision autorisant l'interception et la réalité des propos échangés s'est développé, tant sur le plan quantitatif – malgré la lourde charge de travail ainsi induite – que qualitatif avec le recours à la méthode de l'audition des services. Ce renforcement du contrôle *a posteriori* a permis à son tour le développement des « préconisations » adressées directement aux services, tendant à l'interruption de telle ou telle interception, et généralement acceptées et mises en œuvre par ces derniers sans qu'il soit nécessaire de recourir à l'instrument de la « recommandation » adressée au Premier ministre.

En poursuivant sa politique de dialogue avec les services, et en enrichissant la panoplie de ses méthodes de contrôle, la Commission espère ainsi avoir contribué en 2008 à maintenir l'équilibre toujours délicat entre la protection des libertés et les exigences de la sécurité 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 :

Membres de la Commission :

- Président : Jean-Louis DEWOST, président de section honoraire au Conseil d'État, nommé 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)

- Membre parlementaire – Sénat : Hubert HAENEL, sénateur (UMP) du Haut-Rhin, désigné le 4 juillet 2007 par le président du Sénat en remplacement du sénateur Jacques BAUDOT décédé, puis le 15 octobre 2008 en qualité de membre parlementaire à titre personnel

- Membre parlementaire – Assemblée nationale : Daniel VAILLANT, député (PS) de Paris, désigné le 1<sup>er</sup> août 2007 par le président de l'Assemblée nationale

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

- Rémi RÉCIO, délégué général depuis sa nomination en date du 2 mai 2007

- François COUDERT, chargé de mission depuis sa nomination en date du 5 novembre 2007

Le secrétariat est assuré par Nathalie BRUCKER et Marie-Josée MASSET.

Christophe GERMIN 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
- Daniel VAILLANT, député de Paris, 1<sup>er</sup> août 2007

Représentants du Sénat :

- Marcel RUDLOFF, sénateur du Bas-Rhin, 17 juillet 1991
- Jacques THYRAUD, sénateur du Loir-et-Cher, 26 mars 1992
- Jacques GOLLIET, sénateur de Haute-Savoie, 22 octobre 1992
- Jean-Paul AMOUDRY, sénateur de Haute-Savoie, 14 octobre 1995
- Pierre FAUCHON, sénateur du Loir-et-Cher, 18 septembre 1998
- André DULAIT, sénateur des Deux-Sèvres, 6 novembre 2001
- Jacques BAUDOT, sénateur de Meurthe-et-Moselle, 26 octobre 2004
- Hubert HAENEL, sénateur du Haut-Rhin, 4 juillet 2007, en remplacement du sénateur Jacques BAUDOT décédé, puis le 15 octobre 2008 en qualité de membre parlementaire de la Commission à titre personnel

## 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, modifiée à plusieurs reprises, la dernière fois par la loi n° 2006-64 du 23 janvier 2006.

Conformément à l'article 1<sup>er</sup> de son règlement intérieur, « la Commission se réunit à intervalles réguliers à l'initiative de son président; elle peut également être réunie à la demande d'un de ses membres ». Entre les réunions de la commission plénière, le président dispose d'une habilitation permanente à l'effet de formuler les avis dès lors que la demande d'interception ne pose pas de questions nouvelles par rapport à la jurisprudence établie.

En application de l'article 15 de la loi, la Commission 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; elle peut à tout moment adresser au Premier ministre une recommandation tendant à ce qu'une interception soit interrompue.

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 en outre chargée, en application de l'article 6 de la loi n° 2006-64 du 23 janvier 2006 relative à la loi contre le terrorisme, du contrôle des demandes de communication des données prévues par l'article L. 34-1-1 du Code des postes et des communications électroniques.

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 2008 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 en 2008 se sont élevés à 563 687 euros dont 486 555 euros pour les dépenses du titre II (dépenses de personnel) et à 77 132 euros pour les dépenses de fonctionnement.

Les crédits du BOP CNCIS sont destinés en priorité à permettre le fonctionnement continu de la CNCIS en toute sécurité. 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 classifiés 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 qui lui soit propre pour assurer des déplacements discrets et sûrs, notamment pour effectuer des visites de contrôle. Elle est enfin tenue à la publication d'un rapport annuel.

La CNCIS est partie prenante aux travaux menés par les services du Premier ministre sur la mesure de la performance en matière de gestion budgétaire. Elle a ainsi poursuivi en 2008 d'importants travaux de rationalisation financière au sein desquels on peut, à titre d'exemple, citer la mutualisation informatique avec les services du Premier ministre (la nouvelle adresse électronique de la Commission donnée en page 2 en constituant l'illustration).

## Relations extérieures

La CNCIS a reçu, le 26 juin 2008, la visite d'une délégation du comité « R » du royaume de Belgique.

Bien que sa composition, et surtout sa position institutionnelle, soient sensiblement différentes de celle de la CNCIS, la fonction d'autorité indépendante de contrôle du renseignement exercée par le comité « R » a permis de procéder à de très intéressants échanges de vues.

Ces travaux ont fait apparaître qu'au-delà des différences « systémiques » entre la Belgique et la France, un point de convergence existait entre ces deux autorités de contrôle, à savoir la nature de ce contrôle et l'esprit dans lequel il est exercé. En effet, à l'image du contrôle pratiqué par la CNCIS, le contrôle du comité « R » intègre les principes de **proportionnalité** et de **subsidiarité**.

# Le contrôle des interceptions de sécurité (loi n° 91-646 du 10 juillet 1991)

## 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'interceptions. 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. Il a été confirmé en 2008 par le Pre-

mier ministre lui-même comme pratique « la mieux à même de répondre à l'objectif de protection efficace des libertés poursuivi par le législateur ».

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 au Premier ministre de décider de les interrompre, ou préconise directement aux Services cette 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 des interceptions à un instant donné 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 (1996-2007).

**Tableau récapitulatif de l'évolution des contingents d'interceptions prévus par l'article 5 de la loi du 10 juillet 1991**

	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>

La modification de la jurisprudence de la Commission interprétant désormais ce contingent comme se référant à un nombre maximum de « cibles » devrait permettre de ne pas l'augmenter à brève et moyenne échéance.

#### **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 adéquation avec le motif légal. Ce point, ainsi que les critères d'appréciation des motivations, seront repris dans la deuxième partie du rapport, consacrée à la « jurisprudence de la Commission ».

À cet effet, le cadre des imprimés de demandes a été revu en 2006 et à nouveau en 2008 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 pour autant être perçus comme un carcan dont on ne pourrait sortir, par exemple en présentant spontanément des informations complémentaires indispensables à l'appréciation de la demande.

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 (avocats ou journalistes par exemple).

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. Ceci sera développé dans la deuxième partie du rapport.

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, dès lors qu'elles ne tombent pas sous le coup de la loi, ne justifient pas en tant que tels une demande d'interception s'ils ne comportent aucune menace immédiate pour l'ordre public républicain, matérialisée par exemple par un appel ou un encouragement à la violence. De même, elle veille à ce que les interceptions, en ce qu'elles sont parfois concomitantes d'action sur le terrain, ne portent pas atteinte à la liberté de manifestation.

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

Le président de la CNCIS peut demander les éléments d'informations complémentaires qui lui sont nécessaires pour fonder l'avis de la Commission. Il formule également les observations qu'il juge utiles sur la pertinence du motif invoqué, procédant le cas échéant à des propositions de substitution 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 par une restriction au cas par cas de la durée de la mesure dont le maximum est de quatre mois<sup>1</sup>, par

---

1) Une différenciation des délais a été instaurée par voie jurisprudentielle : deux mois pour une cible encore non totalement identifiée, un mois en cas de risque de récurrence d'une infraction criminelle déjà commise, délai *ad hoc* calé sur un événement prévu à date fixe, etc.

l'instruction donnée d'exclure certaines parties strictement privées des conversations des transcriptions (appelées « productions ») et par des demandes de bilans circonstanciés avant l'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, mise en place de forces de l'ordre, etc.).

## Le contrôle en aval

### Données chiffrées et commentaires

#### • *Évolutions 2007-2008*

5935 interceptions de sécurité ont été sollicitées en 2008 (4330 interceptions initiales et 1605 renouvellements). Le caractère inchangé du contingent depuis juin 2005 explique cette quasi-stabilité par rapport à 2007.

S'agissant des interceptions initiales, 1 095 de ces 4330 demandes ont été présentées selon la procédure dite d'urgence absolue, soit 25 % de ces demandes (23 % en 2007). Il convient ici de préciser que 621 de ces 1 095 urgences absolues ont été constituées d'urgences techniques, soit 56,7 % des urgences (54,5 % en 2007). Force est de constater que ce dernier dispositif permet d'éclairer l'augmentation du nombre de demandes présentées en urgence absolue.

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. Puis, pour répondre au souci des services identifiant en cours d'interception un autre numéro utilisé concurremment par la même cible, ont été également acceptées des interceptions en urgence de ce second numéro, toujours après examen préalable de la Commission. Elles disparaîtront des statistiques en 2009 suite au passage du contrôle par ligne au contrôle par cible.

Cette augmentation constante des urgences absolues pèse de manière significative sur l'organisation de la Commission qui assure un contrôle *a priori* de ces demandes selon une permanence de type parquet du procureur de la République près un tribunal de grande instance. L'un des objectifs prioritaires de cette permanence est de traiter chaque demande d'urgence absolue dans un délai inférieur à une heure. Durant l'année 2008, la Commission a toujours respecté cet objectif.

Au final, si l'on impute à ce chiffre global des demandes d'interceptions (initiales et renouvellements) les 29 avis négatifs donnés par la Commission lors des demandes initiales et des demandes de renouvellement, tous suivis par le Premier ministre, ce sont donc 5906 interceptions de sécurité qui ont effectivement été pratiquées au cours de l'année 2008.

Pour ce qui concerne les motifs au stade des demandes initiales, c'est toujours la criminalité organisée qui reste le premier motif des demandes initiales avec 59 % du total (contre 56,5 % en 2007) suivie de la prévention du terrorisme avec 26,5 % (contre 31 % en 2007) et la sécurité nationale 13 % (contre 11,5 % en 2007). Pour ce qui concerne les renouvellements, on note que c'est la sécurité nationale qui occupe la première place avec 47 %, suivie de la prévention du terrorisme (38 %) et de la criminalité et de la délinquance organisées (14 %).

Au total, demandes initiales et renouvellements confondus, c'est la prévention de la criminalité organisée qui, cette année encore, se détache nettement avec 47 %, suivie de la prévention du terrorisme (29,5 %) et la sécurité nationale (22 %). Ces trois motifs représentent 98,5 % du total 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/défavorable), le nombre d'observations a encore crû, passant de 1 090 en 2007 à 1 239 en 2008 dont 100 demandes de renseignements complémentaires et 254 limitations de la durée d'interception sollicitée. Les avis défavorables, comptés dans les observations, sont en baisse : 29 (19 concernant les demandes initiales et 10 les demandes de renouvellement), tous suivis par le Premier ministre. Cette baisse apparente doit toutefois être nuancée par le recours par la Commission, au cours de l'année 2008, à deux « techniques d'observation » qui peuvent s'apparenter à « l'avis négatif » :

- la recommandation adressée au Premier ministre visant à l'interruption de l'interception en cours d'exploitation qui résulte de l'examen exhaustif des « productions » (transcriptions des interceptions) résultant d'une interception. Il y a été fait recours à 12 reprises en 2008. Elles ont toutes été suivies par le Premier ministre ;
- la « préconisation d'interruption » adressée par la Commission au service utilisateur en cours d'exploitation. Elle résulte du même examen des « productions » et procède d'un dialogue constructif mené directement avec le service. Cette technique a conduit les services utilisateurs à « abandonner » 28 interceptions en 2008.

De fait, si l'on additionne avis négatifs, recommandations d'interruption adressées au Premier ministre et « préconisations d'interruption » adressées directement aux services utilisateurs, le nombre de cas où une interception de sécurité n'a pas été réalisée ou poursuivie conformément au positionnement de la Commission s'établit à 69, ce qui permet de nuancer la baisse des avis négatifs proprement dits (68 en 2007 ; 29 en 2008).

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 » est, en aval, le moyen privilégié pour s'as-

surer 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 » inauguré en 2005 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 » de 172 lignes interceptées en 2008 ont-elles été examinées et la Commission a recommandé la cessation d'interception de douze lignes. Elle a été suivie dans tous les cas par le Premier ministre. À ce chiffre, il convient d'ajouter les 28 « préconisations d'interruption » d'interceptions en cours, directement adressées aux chefs de services et toutes suivies d'effet. La diminution constante relevée plus haut du nombre d'avis négatifs *a priori* est donc compensée très largement par l'augmentation sensible du nombre d'interruptions d'interceptions en cours.

Un nouveau type de démarche auprès du Premier ministre est également apparu dans le cadre du contrôle en aval : il s'agit d'une lettre annonçant qu'une recommandation d'interruption de l'écoute pourrait être envoyée à bref délai si l'incertitude sur l'adéquation entre le motif invoqué et la réalité des propos échangés devait se poursuivre. Une dizaine de courriers a été ainsi adressée au Premier ministre au cours de l'année 2008. Un tel « avertissement » sortant tel ou tel dossier de son anonymat administratif, permet au Premier ministre d'interroger les Services sur une base concrète, et renforce ainsi, au niveau politique, le dialogue déjà amorcé par la Commission à son niveau avec ces mêmes Services, au cours de ces dernières années.

Enfin, la Commission fait désormais appel à la technique de l'audition en séance plénière d'un haut responsable d'un service de renseignement dans des dossiers où le suivi des productions ne suffit plus à établir son intime conviction.

Au total, avec 5906 interceptions accordées en 2008 contre 6000 en 2007, on constate à nouveau que les interceptions de sécurité demeurent, au regard de vecteurs de communications électroniques en constante augmentation, la mesure d'exception voulue par la loi.

## Tableaux annexes

### Les demandes initiales d'interception

#### État des demandes initiales d'interception (2007 et 2008)

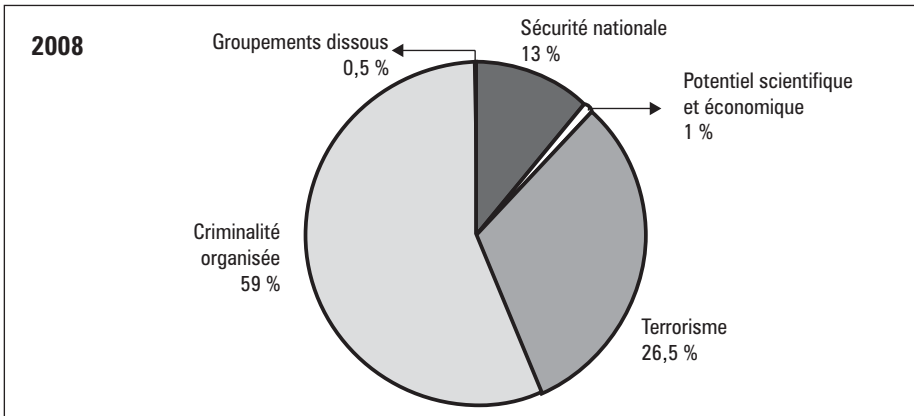
	Demandes initiales		Dont urgence absolue		Accordées	
	2007	2008	2007	2008	2007	2008
<b>Totaux</b>	4 215	4 330	964	1 095	4 173	4 311

#### État comparatif des demandes initiales sur cinq ans

	2004	2005	2006	2007	2008
Sécurité nationale	548	625	622	479	567
Potentiel scientifique et économique	66	43	47	52	38
Terrorisme	1 292	1 468	1 330	1 295	1 138
Criminalité organisée	1 881	2 006	2 195	2 381	2 565
Groupements dissous	0	2	9	8	22
<b>Totaux</b>	<b>3 787</b>	<b>4 144</b>	<b>4 203</b>	<b>4 215</b>	<b>4 330</b>

### Demandes initiales

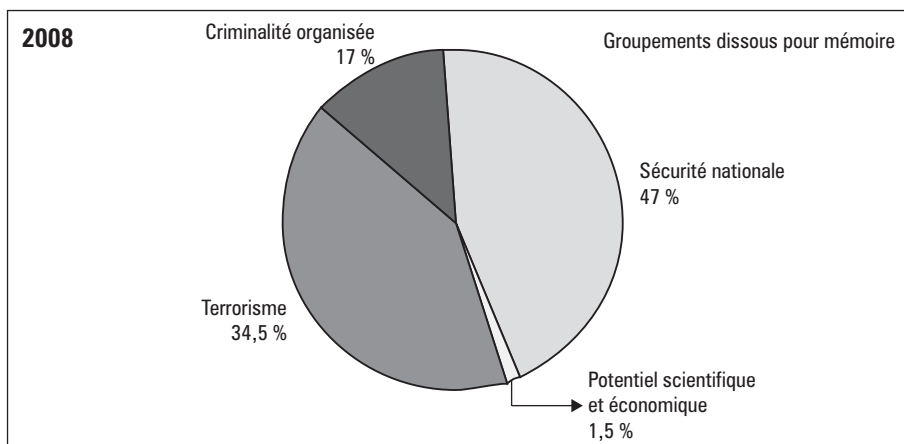
#### Répartition des motifs



## Les renouvellements d'interception

### Répartition des motifs en 2008

Sécurité nationale	Potentiel scientifique et économique	Terrorisme	Criminalité organisée	Groupements dissous	Total « demandés »	Total « accordés »
754	23	551	275	2	1 605	1 595



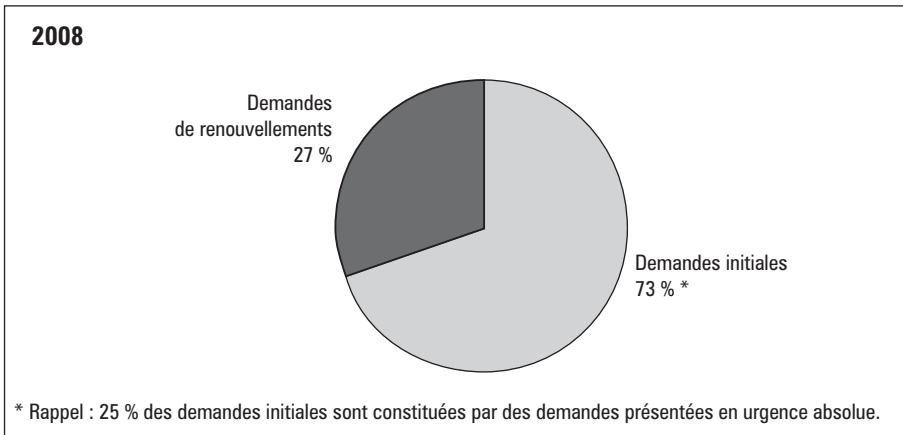
### État comparatif des demandes de renouvellements sur cinq ans

	2004	2005	2006	2007	2008
Sécurité nationale	629	624	735	793	754
Potentiel scientifique et économique	36	42	28	20	23
Terrorisme	1 052	848	794	779	551
Criminalité organisée	201	182	243	251	275
Groupements dissous	0	1	9	7	2
<b>Total</b>	<b>1 918</b>	<b>1 697</b>	<b>1 809</b>	<b>1 850</b>	<b>1 605</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	
2007	2008	2007	2008	2007	2008
3 251	3 235	964	1 095	1 850	1 605



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

	2004	2005	2006	2007	2008
Demandes initiales d'interceptions	3 787	4 144	4 203	4 215	4 330
Dont « urgence absolue »	633	854	714	964	1 095
Demandes de renouvellements	1 936	1 738	1 825	1 850	1 605
<b>Total</b>	<b>5 723</b>	<b>5 882</b>	<b>6 028</b>	<b>6 065</b>	<b>5 935</b>

### Répartition entre interceptions et renouvellements accordés

#### Interceptions accordées en 2008

Interceptions initiales	Renouvellements	Total
4 311	1 595	5 906

## Le contrôle de l'exécution

Celui-ci porte sur trois domaines :

- l'enregistrement, la transcription et la durée des interceptions ;
- les visites sur le terrain ;
- 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 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 dix jours]. » En application de cette disposition, en début d'année civile, le directeur du GIC atteste de la conformité logicielle du parc informatique de tous 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 retenues 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 31 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 en permanence aux avancées technologiques incessantes dans le domaine des communications électroniques qui constituent chaque fois autant de défis à relever (citons en l'espace d'une décennie, la téléphonie mobile, le SMS, le mail, l'internet, le dégroupage et la multiplication des opérateurs).



Conformément à une recommandation prise par la Commission en 1996, le GIC a entrepris dès 1997 la mise en place de centres locaux de regroupement des interceptions, sortes de GIC déconcentrés répondant aux normes de 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.

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

### **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, huit visites de centres d'exploitations ont été effectuées cette année. À chacune de ces visites, les représentants de la CNCIS dressent un inventaire des pratiques et procédures mises en œuvre par les services pour l'application 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, 30 particuliers ont saisi par écrit la CNCIS. Une minorité des courriers concernait des demandes de renseignements sur la législation. La majorité, constituée de réclamations, a donné lieu au contrôle systématique auquel il est procédé lorsque le demandeur justifie d'un intérêt direct et personnel à interroger la Commission sur la légalité d'une éventuelle interception administrative. Il convient de préciser que les agents de la Commission ont traité un chiffre d'appels téléphoniques

bien supérieur à celui des saisines par courrier. Ces contacts préalables ont le plus souvent permis de prévenir des courriers ultérieurs inappropriés lorsqu'il s'agit d'appels malveillants, de problèmes relevant de la saisine de l'autorité judiciaire (soupçons d'écoutes illégales à caractère privé) ou enfin de dysfonctionnements techniques classiques; il a également permis de réorienter les demandeurs vers les services ou autorités compétents.

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 1<sup>er</sup> 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 nature 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 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 :

- 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;

– le Conseil d'État, dans un arrêt du 28 juillet 2000, a rejeté le recours d'un requérant contre la décision du président de la CNCIS refusant de procéder à une enquête aux fins, non de vérifier si des lignes identifiées avaient fait l'objet d'une interception comme la loi lui en donne le pouvoir, mais si la surveillance policière dont l'intéressé se disait victime trouvait sa source dans l'interception de lignes de ses relations.

### **Les avis à l'autorité judiciaire prévus à l'article 17 alinéa 2**

Au cours de l'année 2008, 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**

En vertu des articles R. 226-1 à R. 226-12 du Code pénal, le Premier ministre est compétent pour accorder les autorisations de fabrication, d'importation, d'exposition, d'offre, de location, de vente, d'acquisition ou de détention de matériels permettant de porter atteinte à l'intimité de la vie privée ou au secret des correspondances. Délégation a été donnée au secrétaire général de la défense nationale (SGDN) pour signer au nom du Premier ministre les autorisations, refus ou retraits d'autorisation. Ces signatures interviennent après avis d'une Commission consultative à laquelle participe la CNCIS.

Le nouveau régime de contrôle, 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. 34-38; rapport 2005, p. 31-33). Il traduit une vision libérale quant à la mise sur le marché d'appareils dont la liste initiale a été réduite, vision assortie d'une logique de vigilance quant à l'utilisation finale de ces appareils (*cf.* rapport 2004, p. 38).

Les règles de commercialisation ont été allégées par le nouveau dispositif réglementaire, mais pour autant cette facilitation de l'accès au marché n'a pas induit une inflexion dans la qualification du caractère « sensible » de ce type de matériel par les pouvoirs publics.

Ainsi, le décret 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 stra-

tégiques en France – *Recueil Dalloz* 2006, p. 218) soumet au principe de l'autorisation préalable l'investissement d'un État (intra ou extracommunautaire) portant sur « les matériels conçus pour l'interception des correspondances et la détection à distance des conversations autorisés au titre de l'article 226-3 du Code pénal ».

La Commission consultative prévue à l'article R. 226-2 du Code pénal s'est réunie six fois en 2008. 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 CNCIS;
- un représentant de l'Agence nationale des fréquences;
- deux personnalités désignées en raison de leur compétence par le Premier ministre.

En 2008, la Commission a rendu 406 décisions ventilées comme suit :

- 273 décisions d'autorisation initiale;
- 95 décisions de renouvellement d'autorisation;
- 38 décisions d'ajournement;
- 0 décision de refus ou de retrait;
- 24 décisions de mise « hors champ » de l'examen pour autorisation.

On relèvera cette année encore (*cf.* rapport 2005, p. 32; rapport 2007, p. 26) 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.

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 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.



---

# Le contrôle des opérations de communication des données techniques (loi n° 2006-64 du 23 janvier 2006)

Concernant le contrôle des opérations de communications des données techniques, 2008 aura constitué la première année « pleine » d'exercice de ce contrôle.

En effet, créé par la loi du 23 janvier 2006, le droit pour certains services d'obtenir sur simple réquisition administrative la communication des données techniques afférentes aux communications électroniques pour la seule prévention du terrorisme avait vu le jour dans les faits le 2 mai 2007, et le précédent rapport d'activité n'avait pu en rendre compte que de façon nécessairement partielle.

Il est à noter que ce dispositif, initialement prévu pour une durée de trois années, a été prorogé jusqu'au 31 décembre 2012 par la loi n° 2008-1245 du 1<sup>er</sup> décembre 2008.

## Présentation du dispositif

L'article 6 de la loi n° 2006-64 du 23 janvier 2006 « relative à la lutte contre le terrorisme et portant diverses dispositions relatives la sécurité et aux contrôles frontaliers », adoptée dans un contexte marqué par l'hy-perterrorisme, a octroyé le droit pour certains services impliqués dans

la prévention du terrorisme d'obtenir sur simple réquisition les données techniques afférentes à une communication électronique, autrement et plus simplement dit, d'avoir accès au « contenant » d'une telle communication (facture détaillée, identification des numéros appelés ou appelants, géolocalisation des terminaux utilisés) sans avoir accès au « contenu » de celle-ci (c'est-à-dire la conversation, l'échange de correspondances proprement dit). Ce nouveau droit d'accès constitue un outil d'enquête précieux pour les services, notamment parce qu'il permet d'établir le « relationnel » d'une personne dès lors qu'elle est suspectée de menées terroristes.

Quoique moins intrusive dans le secret des correspondances, cette mesure est en revanche attentatoire d'autres droits des citoyens (droit à l'intimité de la vie privée, liberté d'aller et venir). C'est la raison pour laquelle le législateur a prévu un certain nombre de garanties, garanties au respect desquelles la Commission nationale de contrôle des interceptions de sécurité attache beaucoup d'importance et consacre une part non négligeable de ses activités.

Ainsi, les demandes faites par les services doivent être :

- dûment motivées, et ce au regard de la seule prévention du terrorisme ;
- sollicitées par des « agents individuellement désignés et dûment habilités » ;
- validées préalablement par la « personnalité qualifiée » placée auprès du ministre de l'Intérieur et nommée par la CNCIS pour une durée de trois ans renouvelable, ou par l'un de ses adjoints nommé dans les mêmes conditions.

La loi a par ailleurs conféré à la CNCIS la responsabilité de contrôler *a posteriori* l'activité de la personnalité qualifiée, et le devoir corrélatif de saisir le ministre de l'Intérieur d'une « recommandation » quand elle « constate un manquement aux règles... ou une atteinte aux droits et libertés ».

## Éléments d'ordre statistique

Pour l'année 2008, l'activité a été la suivante :

- 38 306 demandes présentées à la personnalité qualifiée ;
- 34 911 demandes validées ;
- 93 demandes refusées ;
- 3 302 demandes renvoyées au service demandeur pour renseignements complémentaires.

Pour mémoire, au titre de l'année 2007 (sur sept mois), l'activité avait été la suivante :

- 27 701 demandes présentées à la personnalité qualifiée ;
- 25 982 demandes validées ;
- 243 demandes refusées ;

– 1 476 demandes renvoyées au service demandeur pour renseignements complémentaires.

En rythme annuel on peut, d'ores et déjà, observer que l'activité 2008 aura été un peu moins soutenue que l'année 2007, ce qui – peut-être – s'explique par un effet de rattrapage lors de la mise en place en cours d'année d'un dispositif nouveau.

Il convient ici de préciser que le chiffre des demandes validées ne correspond pas au nombre réel de « cibles » concernées. La réalité de l'article 6 est bien loin d'une cardinalité parfaite entre nombre de demandes et nombre de « cibles ». Il n'est en effet pas rare d'observer que plusieurs dizaines de demandes concernent en fait une seule personne soupçonnée de menées terroristes. Ainsi en 2008, ce ne sont donc pas 38 306 personnes qui ont été visées par le dispositif de l'article 6 mais un nombre naturellement inférieur, sans qu'il soit techniquement possible de préciser ce chiffre.

La typologie des demandes formulées par les services révèle que :

- plus de 80 % concernent de simples demandes d'identification d'abonnés, mesures par essence moins attentatoires que les demandes portant sur le trafic observé sur une ligne ;
- une part infinitésimale (0,28 %) a pour objet la géolocalisation du terminal de téléphonie mobile utilisé, mesures dont le caractère attentatoire est le plus marqué puisqu'il permet de connaître les « habitudes de vie » d'une cible au travers de ses déplacements ainsi que son relationnel.

## Étendue et modalités du contrôle exercé par la CNCIS

Au terme de l'année 2008, conformément aux prescriptions de l'article 6 de la loi du 23 janvier 2006, la « personnalité qualifiée » a soumis son deuxième rapport d'activité au président de la Commission, venant ainsi rendre compte de l'exercice de ses missions légales.

Il apparaît que la « personnalité qualifiée » s'est inspirée de l'approche de la Commission concernant les interceptions de sécurité, en privilégiant un dialogue constructif avec les services demandeurs. La personnalité qualifiée a ainsi entendu dès l'origine sortir d'une logique binaire acceptation/refus en sollicitant de façon ponctuelle des renseignements complémentaires avant validation ou refus.

Sur les 38 306 demandes, 93 ont été refusées, soit 0,25 % (chiffre en baisse par rapport à 2007) et 3 302 ont fait l'objet de demandes de renseignements complémentaires, soit 8,6 % du total (chiffre en hausse par rapport à 2007).



Les motifs de refus sont principalement les suivants :

- demandes relatives à des faits déjà commis et/ou faisant l'objet d'enquêtes judiciaires;
- demandes concernant des cibles dont la situation pénale au regard du Code de procédure pénale impose de prendre d'autres mesures;
- demandes relatives à des faits insusceptibles en l'état de constituer des menées terroristes.

Les motifs ayant conduit à une demande de renseignements complémentaires au service demandeur sont notamment les suivants :

- insuffisante implication personnelle de la cible dans des menées à caractère terroriste;
- non-respect des principes de proportionnalité et/ou de subsidiarité;
- contradiction de motifs au sein de la demande;
- absence de précisions sur le mouvement d'appartenance de la cible.

La CNCIS a par ailleurs exercé sa mission de contrôle des activités de la personnalité qualifiée de la façon suivante :

- En poursuivant un dialogue prenant la forme de réunions bimensuelles avec la personnalité qualifiée, lesquelles permettent d'évoquer les difficultés rencontrées par celle-ci dans l'exercice de ses missions et d'expliquer la jurisprudence de la Commission. Ces réunions assurent de fait une unité de jurisprudence tant dans le domaine des interceptions de sécurité que dans celui de l'article 6. Chaque réunion est l'occasion de faire quelques observations à la personnalité qualifiée qui en tient compte par la suite lors de l'examen de nouvelles demandes.

- En exerçant un « contrôle gradué » sur chaque demande validée par la personnalité qualifiée, modulant le seuil de l'exigence de la Commission quant à la qualité de la motivation en fonction du caractère plus ou moins intrusif de la prestation sollicitée au regard des libertés individuelles.

- En adressant à la personnalité qualifiée des notes-cadres sur certains sujets en lien avec l'actualité des demandes, par exemple sur le traitement des menaces d'attentat, lesquelles sont parfois susceptibles de constituer des infractions autonomes justifiant une approche judiciaire exclusive de tout recours à l'article 6, ou encore sur le régime des communications téléphoniques autorisées en milieu pénitentiaire. La délimitation des frontières entre la « prévention du terrorisme » d'une part, et la prévention des atteintes à la sécurité nationale et la criminalité organisée d'autre part, a également fait l'objet d'éclaircissements, la Commission entendant veiller rigoureusement au respect du champ légal d'application de ce mécanisme nouveau, à savoir la seule prévention du terrorisme.

- En adressant quatre recommandations écrites au ministre de l'Intérieur telles que prévues à l'article L. 34-1-1, 5<sup>e</sup> alinéa du Code des postes et communications électroniques. Ces quatre recommandations

avaient principalement pour objet de souligner que la preuve de l'implication directe et personnelle d'une personne dans des activités participant de menées terroristes n'est pas rapportée dans l'hypothèse où elle aurait seulement fait connaître « être en possession d'informations sur des menaces d'attentats imminents » ou d'informations susceptibles de permettre l'identification d'un terroriste présumé. En l'état de cette seule motivation, tout dénonciateur ou informateur serait susceptible de voir analysées ses communications, ce qui n'est pas conforme à l'objectif poursuivi par le législateur.

- En adressant cinq demandes d'éclaircissement à la personnalité qualifiée, telles que prévues à l'article R. 10-20, 2<sup>nd</sup> alinéa du Code des postes et communications électroniques. Ces cinq demandes avaient principalement pour objet de s'assurer du respect du principe de la séparation des pouvoirs en vérifiant que l'article 6 n'avait pas été utilisé alors qu'une enquête judiciaire était en cours.



Deuxième partie

---

# **JURISPRUDENCE DE LA COMMISSION**



Après 17 années d'activité soutenue dans plusieurs compositions différentes, et sous trois présidences successives, les prises de position de la Commission (avis et recommandations) constituent un *corpus* de jurisprudence qui mérite désormais d'apparaître en tant que tel dans le rapport annuel.

Jusqu'à présent, cette jurisprudence était présentée sous l'intitulé « Observations sur les motifs légaux d'interception », dans la partie « Études et documents ». Il a paru plus approprié de réserver cette partie (devenue troisième partie du rapport annuel) aux sources « externes » à la Commission, même si elles font partie de son environnement juridique. Cette nouvelle deuxième partie du rapport reprendra donc l'état de la jurisprudence de la Commission en ce qui concerne les quatre principaux motifs légaux d'interception. Elle est précédée d'une réflexion horizontale de la Commission sur la motivation des demandes en général.

## La qualité de la motivation des demandes d'interception

Chaque semaine, la Commission est amenée à donner son avis sur plus d'une centaine de demandes d'interception de sécurité ; en outre, chaque jour, elle statue en urgence sur cinq à dix demandes.

C'est la **motivation** de ces demandes qui constitue la **base du contrôle de légalité** de celles-ci.

Elle doit donc être :

- suffisante,
- pertinente,
- et sincère.

### Une motivation suffisante

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

- En quantité

Trois lignes ne suffisent pas. Elles ne permettent pas de cerner la personnalité de la cible, de développer un minimum les soupçons qui pèsent sur elle, et d'expliquer la nature et la gravité du danger qu'elle fait courir à la sécurité de l'État et aux citoyens. Dans neuf cas sur dix, les « renseignements complémentaires » fournis à la demande de la Commission emporteront la conviction de cette dernière qui déplore dès lors cette regrettable insuffisance initiale d'information.

- En qualité

La motivation doit absolument :

- faire ressortir l'implication personnelle de la cible ;
- ne pas se référer à un comportement purement hypothétique de celle-ci ;
- ne pas être tournée exclusivement vers le passé.

Quelques exemples – volontairement imprécis – illustreront ces critères.

La référence au milieu familial ou professionnel dans lequel évolue la cible ne suffit pas.

Personne n'est responsable de sa famille, et on peut parfaitement avoir de « mauvaises fréquentations » sans le savoir... surtout si elles font partie du milieu naturel dans lequel on évolue. On ne peut ainsi reprocher à un diplomate étranger de rencontrer d'autres diplomates catalogués comme faisant partie d'un service de renseignement... ce qui n'est pas inscrit sur leurs visages. Le médecin chargé de collecter des fonds pour une association charitable n'est pas nécessairement au courant du détournement de ces fonds au profit d'une entreprise criminelle ou terroriste.

Le directeur d'une entreprise dont les produits font l'objet de contrefaçons sur la base de fausses licences dont on dit qu'elles ont été distribuées « à son insu » ne peut faire légalement l'objet d'une interception, même si la lutte contre la contrefaçon au titre de la protection contre la criminalité organisée est en soi un objectif louable.

## **Une motivation pertinente**

Les soupçons qui pèsent sur la cible doivent nécessairement être en relation avec le motif.

Ainsi, le fonds d'investissement étranger qui « fait son marché » tous azimuts dans l'Hexagone dans le secteur alimentaire, comme dans le secteur du petit matériel électrique, ne peut être suspecté d'atteinte « aux éléments essentiels de notre potentiel scientifique et économique », au motif qu'il « pourrait » ainsi s'intéresser aux secteurs sensibles énumérés par le décret du 30 décembre 2005 relatif au contrôle des investissements étrangers en France.

Ici, la non-pertinence du motif rejoint son insuffisance due au caractère hypothétique de la menace.

De même, la surveillance du marché d'un produit industriel, fût-il sensible, ne constitue pas une motivation pertinente – ni d'ailleurs suffisante – dès lors qu'il n'existe aucun indice de l'intention de nuire à notre « potentiel scientifique et économique », l'existence simplement supposée d'un abus de position dominante relevant de la mise en œuvre des remèdes prévus par le droit de la concurrence.

## Une motivation sincère

L'insincérité du motif allégué est à l'évidence le cas le plus grave. Dans sa forme extrême, à savoir le mensonge caractérisé et délibéré, un tel comportement a pour conséquence la remise en cause de la légalité même de l'interception consentie par hypothèse par le Premier ministre, suite à l'avis favorable de la Commission lui-même émis sur la foi d'informations mensongères.

La Commission n'a heureusement jusqu'à présent pas constaté de telles formes d'insincérité « absolue ».

Elle a, en revanche, attiré l'attention du Premier ministre sur des cas d'insincérité « relative ».

Par exemple, s'agissant de la sécurité nationale ou de la protection du potentiel économique, il est arrivé que la motivation se réfère à des marchés situés dans des zones géographiques « sensibles » vraisemblablement pour emporter la conviction de la Commission, alors que le contrôle des productions a ensuite fait apparaître que la cible développait son activité sur des marchés on ne peut plus « classiques ». Cette manière d'« aggraver le cas » de la cible est une forme d'insincérité.

Dans un autre ordre d'idées, la demande d'interception visant des milieux extrémistes en rébellion contre l'ordre établi pourra être « pimantée » de références à des actes violents commis par ces mêmes milieux dans le passé pour « colorer » en menace terroriste une manifestation politique annoncée qui relève davantage de l'ordre public et de sa protection par les forces de l'ordre.

Tenter de cette manière de contourner les principes de proportionnalité ou de subsidiarité qui gouvernent la matière de la loi de 1991 constitue une autre forme d'insincérité.

Il y a enfin les « trous de mémoire » des services... C'est un autre type d'insincérité.

Ces formes d'insincérité « relative », heureusement rares, peuvent altérer la relation de confiance qui doit exister entre les Services et la Commission. Il convient donc que la hiérarchie exerce avec vigilance son propre contrôle interne des motifs allégués par ses subordonnés.

\* \* \*

On reprendra maintenant, après ces réflexions d'ordre général, l'analyse de la jurisprudence de la Commission, motif par motif.



## 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 premier du livre troisième 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 libertés 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 1994, p. 17 sqq.), 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 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 institutionnelle voulue par leurs auteurs affectant le lieu et le temps des manifestations, la qualité des autorités ou des symboles républicains visés, sont tels que la sécurité nationale peut être menacée.

- S'agissant de la recherche de renseignements, la personne dont on se propose d'intercepter les correspondances doit être suspectée d'attenter par ses agissements personnels aux intérêts fondamentaux de la Nation. Si les services de renseignements ont, par nature, une mission de collecte de renseignements qu'ils remplissent en utilisant la palette des moyens disponibles, le recours aux interceptions de sécurité connaît certaines limites. En effet, l'atteinte exceptionnelle à la vie privée qu'autorise la loi ne peut être justifiée même dans ce domaine que par la menace directe ou indirecte, actuelle ou future que la personne écoutée est susceptible de représenter pour la sécurité nationale. En l'absence de menace, et quel que soit l'intérêt que représente la cible comme source de renseignement pour le domaine considéré, l'atteinte à la vie privée serait contraire au principe de proportionnalité. 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 sécurité étant appréhendée en un instant donné et dans un contexte géopolitique donné par rapport aux besoins vitaux du pays. La Commission considère ainsi que la sécurité énergétique fait désormais intégralement partie de la sécurité nationale.

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

La sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, 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 « fourre-tout » de ces motifs<sup>1</sup>, 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"<sup>2</sup> ; « [...] il est nécessaire que l'État dispose de moyens d'information et d'action adaptés aux **menaces** résultant de l'internationalisation des activités économiques<sup>3</sup> ».

« 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<sup>4</sup> ».

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 (« puis-

---

1) Assemblée nationale, 2<sup>e</sup> séance, 13 juin 1991, *JO*, p. 3153 ; Sénat du 25 juin 1991 *JO*, p. 2065.

2) *Cf. supra*.

3) François Massot, rapport de la Commission des lois de l'Assemblée nationale, 6 juin 1991, document n° 2088, p. 29.

4) A. Vitu, articles 410-1 sqq, *Jurisclasseur pénal*.

sances 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'article 411-7 du Code pénal (on peut d'ailleurs noter que « la communication de secret de fabrique » 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 directement reprise du Code pénal et renvoie à des infractions précises, doivent d'une part répondre à une suspicion d'atteinte à ce potentiel par une menace vérifiable traduisant une intention de nuire aux intérêts d'une entreprise française 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.

---

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.

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 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 ».

Tout en continuant à considérer que ce texte illustre utilement la notion d'« éléments essentiels », la Commission, à l'occasion de l'examen en 2008 de quelques dossiers concernant des intérêts industriels majeurs, a quelque peu assoupli sa doctrine et n'exclut pas désormais des recours ponctuels aux interceptions de sécurité dans des secteurs ne figurant pas expressément dans le décret de 2005. Elle exige toutefois que l'activité de l'entreprise menacée soit liée à la sauvegarde de notre indépendance nationale<sup>1</sup> ou à la sécurité 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 suivants du Code pénal, la qualification d'une infraction d'acte de terrorisme, au sens de l'article 421-1 du Code pénal, revêt une particulière gravité.

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**.

---

1) Le Conseil constitutionnel a retenu l'exigence constitutionnelle de préservation de l'indépendance nationale, dans sa décision n° 86-207 DC du 26 juin 1986 relative à la privatisation de certaines entreprises publiques.

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, page 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 symbolique de locaux publics ou privés.

Toutefois, pour recevoir la qualification de terroristes, ces actes doivent avoir été commis avec la volonté de troubler gravement l'ordre public par l'intimidation ou la terreur, la gravité du trouble consistant dans la peur collective que l'on cherche à répandre dans la population ou partie de celle-ci afin de promouvoir une cause ou faciliter le succès d'une revendication.

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

L'article 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 communauté de vie à caractère conspiratif) 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 délicate à tracer 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 15 juillet 2008 (*JOCE* du 16 juillet), ainsi que par la position commune 2008/959 PESC du Conseil du 16 décembre 2008 (*JOCE* du 17 décembre), 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 est susceptible comme telle de recevoir une qualification pénale (*cf.* article 113-2 al. 2 du Code pénal : « [...] l'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire ») et entre naturellement dans le champ de ce motif légal d'interception.

## Prévention de la criminalité et de la délinquance organisées

Comme les chiffres l'ont encore montré cette année 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, le déroutement de camions entiers avec leur fret, 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 quatrième du Code de procédure pénale un titre vingt-cinquième 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). 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.* rapport 1994, p. 18; rapport 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 tels que l'OCRB (Office central pour la répression du banditisme).

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 concernaient les formes classiques du banditisme (trafic de stupéfiants, proxénétisme, enlèvement, racket, 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 :

- l'expression « groupe criminel organisé » désigne un groupe structuré de trois personnes ou plus existant depuis un certain temps et agissant de concert dans le but de commettre une ou plusieurs infractions graves pour en tirer directement ou indirectement un avantage financier ou un autre avantage matériel ;
- l'expression « infraction grave » désigne un acte constituant une infraction passible d'une peine privative de liberté dont le maximum ne doit pas être inférieur à quatre ans ou d'une peine plus lourde ;
- l'expression « groupe structuré » désigne un groupe qui ne s'est pas constitué au hasard pour commettre immédiatement une infraction et qui n'a pas nécessairement de rôles formellement définis pour ses membres, de continuité dans sa composition ou de structure élaborée.

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

Pénalement, la circonstance de commission en bande organisée aggrave sensiblement plus les faits que la circonstance de simple réunion. Ainsi, le vol en réunion est puni de sept ans d'emprisonnement et le vol en bande organisée de quinze ans de réclusion criminelle (*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.

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

La Commission entend donc réserver le recours à ce motif légal à des agissements d'une gravité certaine, souvent mais pas nécessairement 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.

Troisième partie

---

# ÉTUDES ET DOCUMENTS



# Présentation ordonnée des textes relatifs aux missions de la Commission

## Première mission : les interceptions

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'entrée en vigueur 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 du même Code :

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

On trouvera ci-dessous le tableau récapitulatif des différents types d'interceptions.

**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 CPP)	Matière criminelle et correctionnelle (peine encourue supérieure à 2 ans)	4 mois	Sans limitation
	Juge d'instruction (article 80-4 CPP)	Recherche des causes de la mort ou de disparitions inquiétantes	2 mois	Sans limitation
	Parquet (sous l'autorité du JLD) (article 74-2-695-36 et 696-21 CPP)	Recherche de personnes en fuite	2 mois	Renouvelable 3 fois en matière correctionnelle Sans limitation en matière criminelle
	Parquet (sous l'autorité du JLD) (article 706-95 CPP)	Criminalité organisée	15 jours	Renouvelable 1 fois
Autres	Administration pénitentiaire sous le contrôle du procureur de la République* (article 727-1 CPP)	Prévention des évasions Sécurité et bon ordre des établissements pénitentiaires ou des établissements de santé habilités à recevoir des détenus	Temps de la détention <i>NB</i> : les enregistrements qui ne sont pas suivis de transmission à l'autorité judiciaire par application de l'article 40 CPP ne peuvent être conservés au-delà d'un délai de 3 mois	Sans objet

(\*) Cette mesure est ici retranscrite dans un effort d'exhaustivité. La notion « d'interception » est toutefois à nuancer en ce que l'article 727-1 dispose que les détenus ainsi que leurs correspondants **sont informés** du fait que les conversations téléphonique peuvent être écoutées, enregistrées et interrompues.

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<sup>er</sup> de la loi de 1991.

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

TITRE I (de la loi n° 91-646 du 10 juillet 1991 consolidée) :  
DES INTERCEPTIONS ORDONNÉES PAR L'AUTORITÉ JUDICIAIRE

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

Code de procédure pénale

Livre I<sup>er</sup> : De l'exercice de l'action publique et de l'instruction

Titre III : Des juridictions d'instruction

Chapitre I<sup>er</sup> : Du juge d'instruction : juridiction d'instruction du premier degré

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

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

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

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

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

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

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



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

Les enregistrements sont placés sous scellés fermés. »

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

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

• 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***

Code de procédure pénale

Livre I<sup>er</sup> : De l'exercice de l'action publique et de l'instruction

Titre II : Des enquêtes de contrôle d'identité

Chapitre I<sup>er</sup> : Des crimes et des délits flagrants

**Article 74-2** – « Les officiers de police judiciaire, assistés le cas échéant des agents de police judiciaire, peuvent, sur instructions du procureur de la République, procéder aux actes prévus par les articles 56 à 62 aux fins de rechercher et de découvrir une personne en fuite dans les cas suivants :

- 1) personne faisant l'objet d'un mandat d'arrêt délivré par le juge d'instruction, le juge des libertés et de la détention, la chambre de l'instruction ou son président ou le président de la cour d'assises, alors qu'elle est renvoyée devant une juridiction de jugement ;
- 2) personne faisant l'objet d'un mandat d'arrêt délivré par une juridiction de jugement ou par le juge de l'application des peines ;
- 3) personne condamnée à une peine privative de liberté sans sursis supérieure ou égale à un an, lorsque cette condamnation est exécutoire ou passée en force de chose jugée. »

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

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

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

Code de procédure pénale (loi n° 2002-1138 du 9 septembre 2002, article 66)

Livre I<sup>er</sup> : De l'exercice de l'action publique et de l'instruction

Titre III : Des juridictions d'instruction

Chapitre I<sup>er</sup> : Du juge d'instruction : juridiction d'instruction du premier degré

Section I : Dispositions générales

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

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

***Les interceptions ordonnées en matière de criminalité et délinquance organisées***

Code de procédure pénale

Livre IV : De quelques procédures particulières

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

Chapitre II : Procédure

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

**Article 706-95** – « Si les nécessités de l'enquête de flagrance ou de l'enquête préliminaire relative à l'une des infractions entrant dans le champ d'application de l'article 706-73 l'exigent, le juge des libertés et de la détention du tribunal de grande instance peut, à la requête du procureur de la République, autoriser l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications selon les modalités prévues par les articles 100 deuxième alinéa, 100-1 et 100-3 à 100-7, pour une durée maximum 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 [...]. »

***Les interceptions prévues par l'article 727-1 du CPP***

Code de procédure pénale

Livre V : Des procédures d'exécution

Titre II : De la détention

Chapitre III : Des dispositions communes aux différents établissements pénitentiaires

**Article 727-1** – Créé par la loi n° 2007-297 du 5 mars 2007 – article 72 *JORF* 7 mars 2007

« Aux fins de prévenir les évasions et d'assurer la sécurité et le bon ordre des établissements pénitentiaires ou des établissements de santé habilités à recevoir des détenus, les communications téléphoniques que les personnes détenues ont été autorisées à passer peuvent, à l'exception de celles avec leur avocat, être écoutées, enregistrées et interrompues par l'administration pénitentiaire sous le contrôle du procureur de

la République territorialement compétent, dans des conditions et selon des modalités qui sont précisées par décret.

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

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

**Article D. 419-3** – Créé par le décret n° 2007-699 du 3 mai 2007 – article 11 *JORF* 5 mai 2007

« Conformément aux dispositions de l'article 727-1, les conversations téléphoniques, à l'exception de celles avec les avocats, peuvent, sous la responsabilité du chef d'établissement, être écoutées, enregistrées et interrompues par le personnel de surveillance désigné à cet effet.

Dans les maisons centrales, les conversations téléphoniques peuvent être enregistrées de façon systématique.

L'information du détenu et de son correspondant relative à ces contrôles est faite au début de la conversation, le cas échéant par un message préenregistré.

Les conversations téléphoniques peuvent faire l'objet d'une interruption lorsque leur contenu est de nature à compromettre l'un des impératifs énoncé au troisième alinéa de l'article D. 419-1.

Les conversations en langue étrangère peuvent être traduites aux fins de contrôle.

La transmission au procureur de la République des conversations susceptibles de constituer ou de faciliter la commission d'un crime ou d'un délit est effectuée immédiatement, au moyen d'une retranscription sur support papier. Si les communications concernent une personne mise en examen, copie en est adressée au juge d'instruction saisi.

Les enregistrements sont conservés pour une durée maximum de trois mois.

Pendant cette durée, seuls le chef d'établissement et les membres du personnel de surveillance qu'il habilite à cet effet peuvent avoir accès à ces enregistrements, sous réserve des dispositions du dernier alinéa.

La destruction des enregistrements qui n'ont pas été transmis à l'autorité judiciaire est effectuée à l'expiration du délai de trois mois sous la responsabilité du chef d'établissement.

Le procureur de la République peut procéder sur place, à tout moment, au contrôle du contenu des enregistrements conservés. Il peut ordonner leur destruction si leur conservation ne lui paraît plus nécessaire, après en avoir informé le chef d'établissement.»

TITRE II (de la loi n° 91-646 du 10 juillet 1991 consolidée) :  
DES INTERCEPTIONS DE SÉCURITÉ

**Article 3** – « Peuvent être autorisées, à titre exceptionnel, dans les conditions prévues par l'article 4, les interceptions de correspondances 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 reconstitution ou du maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées. »

**Article 4** – *modifié par l'article 6 II de la loi 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 pro-

céder 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 utiles. »

TITRE III (de la loi n° 91-646 du 10 juillet 1991 consolidée) :  
DISPOSITIONS COMMUNES AUX INTERCEPTIONS  
JUDICIAIRES ET DE SÉCURITÉ

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



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

**Article 22** – (*modifié par l'article 18 de la loi 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 € d'amende. Les personnes morales peuvent être déclarées responsables pénalement dans les conditions prévues par l'article 121-2 du Code pénal de l'infraction définie au présent alinéa. Les peines encourues par les personnes morales sont l'amende, suivant les modalités prévues par l'article 131-38 du Code pénal. »

**Article 23** – « Les exigences essentielles définies au 12° de l'article L. 32 du Code des postes et des "communications électroniques" et le secret des correspondances mentionné à l'article L. 32-3 du même Code ne sont opposables ni aux juridictions compétentes pour ordonner des interceptions en application de l'article 100 du Code de procédure pénale, ni au ministre chargé des "communications électroniques" dans l'exercice des prérogatives qui leur sont dévolues par la présente loi. »

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

**Article 226-3** – « Est puni des mêmes peines [un an d'emprisonnement et 45 000 euros d'amende] la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente, en l'absence d'autorisation ministérielle dont les conditions d'octroi sont fixées par décret en Conseil d'État, d'appareils conçus pour réaliser les opérations pouvant constituer l'infraction prévue par le deuxième alinéa de l'article 226-15 ou qui, conçus

pour la détection à distance des conversations, permettent de réaliser l'infraction prévue par l'article 226-1 et figurant sur une liste dressée dans des conditions fixées par ce même décret. Est également puni des mêmes peines le fait de réaliser une publicité en faveur d'un appareil susceptible de permettre la réalisation des infractions prévues par l'article 226-1 et le second alinéa de l'article 226-15 du Code pénal lorsque cette publicité constitue une incitation à commettre cette infraction.»

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

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

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

**Article 26** – «Sera punie des peines mentionnées à l'article 226-13<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 (de la loi n° 91-646 du 10 juillet 1991 consolidée) :  
COMMUNICATION DES DONNÉES TECHNIQUES  
RELATIVES À DES COMMUNICATIONS ÉLECTRONIQUES

**Article 27** – «La Commission nationale de contrôle des interceptions de sécurité exerce les attributions définies à l'article L. 34-1-1 du Code des postes et des communications électroniques et à l'article 6 de la loi 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.»

---

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

TITRE V (de la loi n° 91-646 du 10 juillet 1991 consolidée) :  
DISPOSITIONS FINALES

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

## Deuxième mission : les opérations de communications de données techniques (loi 2006-64 du 23 janvier 2006)

### **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 techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications.

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

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

Cette instance peut à tout moment procéder à des contrôles relatifs aux opérations de communication des données techniques. Lorsqu'elle constate un manquement aux règles définies par le présent article ou une atteinte aux droits et libertés, elle saisit le ministre de l'Intérieur d'une recommandation. Celui-ci lui fait connaître dans un délai de quinze jours les mesures qu'il a prises pour remédier aux manquements constatés.

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

**II.** – Après le II de l'article 6 de la loi 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.** À 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 (de la loi n° 91-646 du 10 juillet 1991 consolidée):  
COMMUNICATION DES DONNÉES TECHNIQUES  
RELATIVES À DES COMMUNICATIONS ÉLECTRONIQUES

**Article 27** – « La Commission nationale de contrôle des interceptions de sécurité exerce les attributions définies à l'article L. 34-1-1 du Code des postes et des communications électroniques et à l'article 6 de la loi 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 JASPART 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 (articles 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 (3<sup>e</sup> rapport 1994, p. 19; 7<sup>e</sup> rapport 1998, p. 23; 8<sup>e</sup> rapport 1999, p. 14).

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



## Troisième mission : le contrôle du matériel

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

- **Les dispositions législatives qui définissent et répriment les infractions d'atteinte à la vie privée et au secret des correspondances :**

- article 226-1 du Code pénal : réprimant les atteintes à la vie privée ;
- article 226-15 du Code pénal : réprimant le détournement de correspondance. Ce texte inclut, dans cette notion de détournement, le fait, de mauvaise foi : « d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions » ;
- article 226-3 du Code pénal : réprimant la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente, en l'absence d'autorisation ministérielle dont les conditions sont fixées par décret en Conseil d'État, d'appareils conçus pour réaliser les opérations pouvant constituer l'infraction prévue par l'article 226-15 du Code pénal.

- **Le décret 97-757 du 10 juillet 1997** qui met en œuvre, à la faveur des articles R. 226-1 à R. 226-12 du Code pénal, la procédure d'« autorisation ministérielle » prévue par l'article 226-3 du Code pénal. L'organisation de la Commission consultative placée sous la présidence du 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. 35-38) 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 prévue 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 SGEN 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 complétera 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 effectuée 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 :
  - 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) ;
  - 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 :
  - le fait de ne pas tenir un registre ou de refuser de le présenter aux services enquêteurs (article R. 226-10) ;



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

# Actualité législative et réglementaire

**Loi n° 2008-1245 du 1<sup>er</sup> décembre 2008 visant à prolonger l'application des articles 3, 6 et 9 de la 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**

**Article unique**

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

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

**Décret n° 2008-609 du 27 juin 2008 relatif aux missions et à l'organisation de la direction centrale du renseignement intérieur**

Vu le Code de procédure pénale ;  
Vu le Code de la défense ;  
Vu la loi n° 66-492 du 9 juillet 1966 modifiée portant organisation de la police nationale ;

Vu la loi n° 92-125 du 6 février 1992 relative à l'administration territoriale de la République, notamment son article 4;

Vu le décret n° 79-433 du 1<sup>er</sup> juin 1979 relatif aux pouvoirs des ambassadeurs et à l'organisation des services de l'État à l'étranger;

Vu le décret n° 85-1057 du 2 octobre 1985 modifié relatif à l'organisation de l'administration centrale du ministère de l'Intérieur et de la Décentralisation, notamment son article 5;

Vu le décret n° 98-608 du 17 juillet 1998 modifié relatif à la protection des secrets de la défense nationale;

Vu le décret n° 2004-374 du 29 avril 2004 relatif aux pouvoirs des préfets, à l'organisation et à l'action des services de l'État dans les régions et départements;

Vu l'avis du comité technique paritaire central de la police nationale du 7 avril 2008;

Vu l'avis du comité technique paritaire de l'administration centrale du ministère de l'Intérieur, de l'Outre-Mer et des Collectivités territoriales du 8 avril 2008;

Vu l'avis du comité technique paritaire ministériel du ministère de l'Intérieur, de l'Outre-Mer et des Collectivités territoriales du 9 avril 2008;

Le Conseil d'État (section de l'intérieur) entendu;

Le Conseil des ministres entendu,

Décrète :

### **Article 1**

La Direction centrale du renseignement intérieur a compétence pour lutter, sur le territoire de la République, contre toutes les activités susceptibles de constituer une atteinte aux intérêts fondamentaux de la Nation.

À ce titre :

- a) Elle est chargée de prévenir les activités inspirées, engagées ou soutenues par des puissances ou des organisations étrangères et de nature à menacer la sécurité du pays, et concourt à leur répression;
- b) Elle participe à la prévention et à la répression des actes terroristes ou visant à porter atteinte à l'autorité de l'État, au secret de la défense nationale ou au patrimoine économique du pays;
- c) Elle contribue à la surveillance des communications électroniques et radioélectriques susceptibles de porter atteinte à la sûreté de l'État ainsi qu'à la lutte, en ce domaine, contre la criminalité liée aux technologies de l'information et de la communication;
- d) Elle participe également à la surveillance des individus, groupes, organisations et à l'analyse des phénomènes de société, susceptibles, par leur caractère radical, leur inspiration ou leurs modes d'action, de porter atteinte à la sécurité nationale.

## **Article 2**

La Direction centrale du renseignement intérieur recherche, centralise et exploite tous les renseignements se rapportant aux activités mentionnées à l'article 1<sup>er</sup> et que lui transmettent sans délai tous les services concourant à la sécurité nationale.

Le service chargé, sous l'autorité du préfet de police, de missions de renseignement intérieur concourt à l'activité de la direction centrale du renseignement intérieur.

## **Article 3**

La Direction centrale du renseignement intérieur assure les liaisons nécessaires, dans ses domaines de compétence, avec les services ou organismes concernés, français ou étrangers, sans préjudice des dispositions régissant les organes de coopération policière internationale.

Elle dispose à cet effet d'officiers de liaison à l'étranger.

## **Article 4**

Les services territoriaux de la direction centrale du renseignement intérieur, en métropole et outre-mer, sont placés sous la seule autorité du directeur central.

Les chefs des services territoriaux de la Direction centrale du renseignement intérieur rendent compte de leur action au représentant de l'État territorialement compétent, d'initiative ou à la demande de celui-ci, dans la limite du besoin d'en connaître.

Il peut être créé des services à compétence zonale ou interdépartementale.

## **Article 5**

Tout agent public est tenu de garder le secret sur les activités et l'organisation de la Direction centrale du renseignement intérieur.

## **Article 6**

Le décret n° 82-1100 du 22 décembre 1982 fixant les attributions de la direction de la surveillance du territoire est abrogé.

## **Article 7**

Le Premier ministre, la ministre de l'Intérieur, de l'Outre-Mer et des Collectivités territoriales et la garde des Sceaux, ministre de la Justice, sont responsables, chacun en ce qui le concerne, de l'application du présent décret, qui entrera en vigueur le 1<sup>er</sup> juillet 2008 et sera publié au *Journal officiel de la République française*.



---

# 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 susvisé, 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. 25) 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 des cours et tribunaux

## Jurisprudence européenne

**Cour européenne des droits de l'homme**  
**LIBERTY et autres – Royaume-Uni (N° 58243/00)**  
**Arrêt 1.7.2008 (section IV)**

Arrêt disponible seulement en version anglaise; seul un résumé en français publié par la Cour (note d'information sur la jurisprudence de la cour, n° 110) est par conséquent reproduit ci-après.

*Interception par le ministère de la Défense, sur la base d'un mandat, des communications vers l'extérieur d'organisations œuvrant dans le domaine des libertés civiles : violation*

*En fait* : la loi de 1985 sur l'interception de communication incriminait l'interception volontaire de communications réalisées par voie postale ou au moyen d'un système de télécommunication public. Toutefois, elle habilitait le ministre de l'Intérieur à délivrer des mandats autorisant la surveillance de communications lorsque pareille mesure était jugée nécessaire à la sécurité nationale, à la détection et à la prévention d'infractions graves ou à la sauvegarde des intérêts économiques nationaux. Les mandats en question pouvaient viser les communications intérieures ou extérieures se rapportant à une adresse ou à une personne déterminée et l'article 3 § 2 de la loi prévoyait aussi la délivrance de mandats autorisant l'interception de communications extérieures non spécifiquement liées à une personne ou à une adresse.



L'article 6 de la loi invitait le ministre de l'Intérieur à prendre les mesures qu'il jugerait nécessaires pour prévenir les abus de pouvoir. Il a été indiqué que de telles mesures avaient été prises, mais, pour des motifs de sécurité nationale, le détail de leur contenu n'a pas été divulgué. La loi de 1985 instituait également une juridiction – la commission de recours contre les interceptions de communications (*Interception of Communications Tribunal* – « la CRIC ») – compétente pour connaître des griefs des personnes se prétendant victimes d'une interception de communications et prévoyait la désignation d'un commissaire chargé d'établir des rapports sur les interceptions et de les contrôler.

Les requérantes sont une organisation britannique et deux organisations irlandaises de protection des libertés civiles. Elles alléguaient devant la Cour que, entre 1990 et 1997, leurs communications par téléphone, télécopie et courriel, dont certaines contenaient des informations juridiques couvertes par le secret professionnel et des renseignements confidentiels, avaient été interceptées au moyen d'un dispositif électronique géré par le ministère britannique de la Défense. Elles avaient auparavant contesté la légalité des interceptions alléguées devant la CRIC, le *Director of Public Prosecutions* et la commission des pouvoirs d'enquête (*Investigatory Powers Tribunal* – « la CPE »), mais ces autorités avaient conclu à l'absence d'infraction à la loi de 1985. La CPE avait notamment jugé que le mandat habilitant les autorités à intercepter et analyser des données ainsi que les conditions de réalisation de ces opérations étaient d'une accessibilité et d'une prévisibilité suffisantes au regard de la loi (loi de 1985 a été abrogée par une loi nouvelle).

*En droit* : la simple existence d'une législation autorisant la surveillance secrète de communications crée une menace de surveillance pour tous ceux auxquels on pourrait l'appliquer. Il s'ensuit qu'il y a eu ingérence dans les droits des requérantes. L'article 3 § 2 de la loi de 1985 conférait aux autorités britanniques une latitude pratiquement illimitée pour intercepter des communications entre le Royaume-Uni et une personne située hors du territoire britannique. Les mandats pouvaient porter sur un très large éventail de communications. En théorie, toute personne émettant ou recevant des communications extérieures aux îles britanniques était susceptible de faire l'objet d'une telle mesure à l'époque pertinente. En outre, les autorités avaient une grande liberté dans le choix des communications à lire ou à écouter parmi celles qui avaient été enregistrées.

S'il est vrai que, au cours de la période pertinente, des directives internes, des manuels et des circulaires prévoyaient des mesures de protection contre les abus de pouvoir et que les rapports annuels du commissaire désigné en vertu de la loi de 1985 pour en contrôler la mise en œuvre ont tous indiqué que les « mesures » en question étaient satisfaisantes, leur contenu n'a jamais été précisé par la loi ou rendu public d'une autre manière. Par ailleurs, bien que le Gouvernement ait allégué que la divulgation d'informations sur ces mesures au cours de la période pertinente aurait pu nuire à l'efficacité du système de collecte du ren-

seignement ou constituer une menace pour la sécurité, la Cour relève que de larges extraits du Code de conduite des interceptions de communications sont aujourd'hui librement accessibles au Royaume-Uni, ce qui donne à penser que les autorités pouvaient rendre publics certains aspects du fonctionnement d'un dispositif de surveillance extérieure sans compromettre la sécurité nationale. En définitive, la Cour considère que, faute d'avoir indiqué avec une clarté suffisante l'étendue et les modalités d'exercice du pouvoir discrétionnaire très étendu dont les autorités bénéficiaient en matière d'interception et d'analyse des communications extérieures, le droit interne applicable à l'époque des faits n'offrait pas une protection adéquate contre les abus de pouvoir. En particulier, aucune précision quant à la procédure applicable à l'analyse, au partage, à la conservation et à la destruction des communications interceptées n'a été rendue accessible au public. Il s'ensuit que l'ingérence dans les droits des requérantes n'était pas « prévue par la loi ».

*Conclusion* : violation (unanimité)

Article 41 – Le constat de violation auquel la Cour est parvenue constitue en soi une satisfaction équitable suffisante pour le préjudice moral que les requérantes pourraient avoir subi.

## Jurisprudence française

**Cour de cassation**

**Chambre criminelle**

**Audience publique du mercredi 26 mars 2008**

**N° de pourvoi : 07-88281**

Publié au bulletin **Rejet**

*CRIMINALITÉ ORGANISÉE – Procédure – Interceptions de correspondances émises par la voie des télécommunications – Contrôle du juge des libertés et de la détention – Autorisation écrite – Moment – Portée*

*Si la décision écrite par laquelle le juge des libertés et de la détention autorise, en application des articles 100 et 706-95 du Code de procédure pénale, l'interception de correspondances émises par la voie des télécommunications, doit intervenir avant que la réquisition ne soit délivrée à l'opérateur téléphonique, il n'est pas exigé que l'autorisation ait été transmise préalablement à l'officier de police judiciaire*

*CRIMINALITÉ ORGANISÉE – Procédure – Interceptions de correspondances émises par la voie des télécommunications – Contrôle du juge des libertés et de la détention – Information prévue par l'article 706-95, alinéa 3, du Code de procédure pénale – Étendue – Détermination*

*Les informations données par le procureur de la République au juge des libertés et de la détention, en application de l'article 706-95, alinéa 3, du Code de procédure pénale, portent sur les diligences effectuées et non sur leur contenu*

LA COUR DE CASSATION, CHAMBRE CRIMINELLE, a rendu l'arrêt suivant :

Statuant sur le pourvoi formé par :

– X... Mario,

contre l'arrêt de la chambre de l'instruction de la cour d'appel de PARIS, 6<sup>e</sup> section, en date du 23 novembre 2007, qui, dans l'information suivie contre lui des chefs de direction d'un groupe ayant pour activité le trafic de stupéfiants, importation en bande organisée de stupéfiants, trafic de stupéfiants, association de malfaiteurs en vue du trafic de stupéfiants, a prononcé sur sa demande d'annulation de pièces de la procédure ;

La COUR, statuant après débats en l'audience publique du 11 mars 2008

[...]

Sur le premier moyen de cassation, pris de la violation des articles 706-95, 100,100-1 à 100-5, 171, 173, 591 à 593 du Code de procédure pénale, défaut de motifs, manque de base légale, ensemble excès de pouvoir ;

« en ce que l'arrêt attaqué a refusé d'annuler les réquisitions judiciaires tendant à l'interception de la ligne cellulaire espagnole n° 00... ainsi que les mesures d'enregistrement et de transcription de cette ligne ;

« aux motifs que le 28 juillet 2006, le lieutenant de police Y... en fonction à l'OCRTIS a adressé par fax à 17 heures 49 au procureur de la République un rapport concluant à l'utilité de placer sous écoutes la ligne téléphonique espagnole numéro 00... dont l'utilisateur, susceptible d'être Mario X..., venait de communiquer le numéro à Abdelnouar Z... (tome 2 / D. 46 à D. 49) ; que le même jour, le juge des libertés et de la détention, sur requête du parquet, a autorisé l'interception de cette ligne téléphonique ainsi que l'enregistrement et la transcription des conversations, décision adressée par fax à 18 heures 15 aux enquêteurs (tome 2 / D. 43, D. 44, D. 45) ; que les enquêteurs ont établi à partir de 17 heures 30 un procès-verbal visant la requête du procureur de la République et l'autorisation donnée par le juge des libertés et de la détention, indiquées comme annexées en fin de procès-verbal, et à 18 heures le procès-verbal de réquisition à l'opérateur de téléphonie au visa de la requête du procureur de la République et de l'autorisation d'interception délivrée par le juge des libertés et de la détention, et non de l'ordonnance même du magistrat (tome 4 / D. 1892, D. 1894, D. 1895) ; que les enquêteurs ont enregistré la première conversation à 18 heures 23 (tome 4 / D. 1930) et ont avisé le procureur de la République à 18 heures 30 de la mise en place de la surveillance technique de cette ligne (tome 2 / D. 732) ; que l'article 706-95 du Code de procédure pénale exige que les enquêteurs disposent d'une autorisation du juge des libertés et de la détention avant

de lancer leurs investigations; que c'est en ce sens que s'est prononcé le Conseil constitutionnel dans sa décision du 2 mars 2004 invoquée par le requérant, en rappelant effectivement la nécessité du caractère écrit de l'autorisation; que si comme le stipulent les articles 100 et 100-1 du Code de procédure pénale qui régissent les opérations autorisées par le juge des libertés et de la détention, la décision d'interception est écrite et doit comporter tous les éléments permettant l'identification de la ligne à intercepter, l'infraction objet des poursuites qui motivent le recours à l'interception ainsi que la durée de la mesure, elle n'est pas une décision juridictionnelle; qu'en conséquence, même si elle est écrite et fait l'objet d'une ordonnance, elle n'a pas à être motivée et n'est susceptible d'aucun recours; que c'est dès lors son principe d'existence qui importe et le respect de ses termes par les services auxquels elle est destinée, une telle décision n'ayant pas à être notifiée pour être exécutoire; que le lieutenant de police A..., par procès-verbal du 28 juillet 2006, commencé à 17 heures 30, vise "l'autorisation d'interception", et non l'ordonnance du juge des libertés et de la détention; qu'il mentionne en fin de procès-verbal, sous sa signature, la poursuite d'investigations par la mention "de même suite, annexons au présent la requête du parquet et l'autorisation d'interception du juge des libertés et de la détention", libellé qui n'est pas incompatible avec la transmission intervenue entre-temps de l'ordonnance, à 18 heures 15, dès lors qu'aucune heure de clôture ne figure en fin de procès-verbal; qu'il est constant que les enquêteurs ont, sans se contredire, régulièrement requis l'opérateur de téléphonie dès 18 heures, avant d'avoir en leur possession l'ordonnance, étant précisé que les interceptions ont été actives à 18 heures 23, soit après la réception de l'ordonnance par fax, et ont avisé le procureur de la République de la mise en place de la surveillance technique de cette ligne à 18 heures 30;

« alors, d'une part, que l'autorisation du juge des libertés et de la détention permettant l'interception d'une ligne téléphonique ainsi que l'enregistrement et la transcription des conversations doit être écrite et exister avant la réquisition adressée par l'officier de police judiciaire à l'opérateur téléphonique; qu'en l'espèce, en refusant d'annuler la réquisition adressée à France Télécom à 18 heures, avant que l'autorisation écrite du juge des libertés et de la détention ne lui soit parvenue et sans qu'il résulte ni des pièces de la procédure ni des motifs de l'arrêt attaqué que l'autorisation du juge des libertés et de la détention avait été rédigée avant ladite réquisition, la chambre de l'instruction a entériné l'excès de pouvoir des enquêteurs et violé les textes susvisés;

« alors, d'autre part, que l'excès de pouvoir résultant de la rédaction par un officier de police judiciaire d'une réquisition sans autorisation écrite du juge d'instruction ne saurait être justifié ni par l'annexion d'une autorisation écrite à un procès-verbal, sans qu'il ne soit justifié qu'elle fût antérieure à cette réquisition ni par le fait que les premières intercep-

tions téléphoniques n'ont eu lieu qu'après la réception d'une autorisation écrite par télécopie » ;

Attendu que Mario X..., mis en examen des chefs susvisés à la suite d'une enquête de flagrant délit, au cours de laquelle plusieurs mesures d'interceptions de communications téléphoniques avaient été mises en place, a saisi la chambre de l'instruction d'une requête aux fins d'annulation, notamment, du procès-verbal de mise en place de la surveillance technique, des réquisitions judiciaires, des enregistrements des appels téléphoniques et des actes subséquents, en faisant valoir que les mesures techniques d'interception avaient précédé la décision d'autorisation prise par le juge des libertés et de la détention ;

Attendu que, pour écarter cette demande, l'arrêt prononcé par les motifs repris au moyen ;

Attendu qu'en se déterminant ainsi, et dès lors qu'il y a lieu de distinguer l'autorisation écrite accordée par le juge, de la transmission de ce document aux services de police, et qu'en l'espèce, il n'est pas établi que cette autorisation soit intervenue après que la réquisition a été délivrée à l'opérateur téléphonique, l'arrêt n'encourt pas les griefs du moyen ;

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

Sur le deuxième moyen de cassation, pris de la violation des articles 706-95, 100, 100-1 à 100-5, 171, 173, 591 à 593 du Code de procédure pénale, défaut de motifs, manque de base légale ;

« en ce que l'arrêt attaqué a refusé d'annuler l'autorisation d'interception du juge des libertés et de la détention de la ligne cellulaire espagnole n° 00... ainsi que les procès-verbaux de transcription de cette ligne ;

« aux motifs que l'autorisation du juge des libertés et de la détention vise "l'interception... de la ligne téléphonique espagnole numéro 00... ainsi que l'enregistrement des appels envoyés-reçus sur le territoire national par cette ligne et leur transcription s'ils sont utiles à la manifestation de la vérité" ; que le juge d'instruction, et dans le cadre d'une enquête, le juge des libertés et de la détention, peut, en application des articles 100 et suivants du Code de procédure pénale, ordonner l'interception, l'enregistrement et la transcription des correspondances émises par la voie des télécommunications à destination des lignes téléphoniques localisées à l'étranger dès lors que les interceptions, réalisées à partir de centres internationaux de transit situés en France, portent sur les appels émis depuis le territoire français ; que la formulation générale par l'usage des termes "envoyés-reçus" aurait pu laisser entendre, comme le soutient le requérant, que les appels émis à partir de la ligne de téléphonie mobile espagnole depuis l'étranger pouvaient être interceptés ; que toutefois, l'ajout de la mention "sur le territoire national" vient démontrer que le magistrat a entendu limiter son autorisation aux appels émis et reçus par cette ligne sur le territoire français, la circons-

tance qu'il s'agissait d'une ligne étrangère n'ayant aucune incidence; que le libellé ne comporte donc pas d'irrégularité quant aux conditions dans lesquelles la mesure d'interception devait être mise en place; que de surcroît la réquisition judiciaire adressée par les enquêteurs au directeur de France Télécom porte sur une prestation en deçà de l'autorisation judiciaire accordée puisque le procès-verbal de réquisition du 28 juillet 2006 se limite à une demande d'interception "des appels au départ du territoire national à destination de la ligne cellulaire espagnole" (D. 1895); qu'il en résulte que seules les conversations émises en France à destination de cette ligne, avec renvoi dans les locaux de la DCPJ à Paris 8<sup>e</sup>, ont été enregistrées et transcrites et non celles reçues en France par cette ligne mobile; qu'il importe peu au regard des droits du requérant, que l'opérateur n'ait pas répertorié les numéros appelant la ligne espagnole puisque leur origine nationale était bien circonscrite (D. 1901); que la question de la distinction qu'il ne serait pas possible d'opérer entre les appels émis depuis la ligne téléphonique mobile espagnole et ceux reçus sur cette ligne est donc sans intérêt au vu du procès-verbal de réquisition dépourvu d'ambiguïté quant à l'origine des conversations interceptées;

« alors, d'une part, que le juge des libertés et de la détention peut, en application des articles 706-95 et 100 et suivants du Code de procédure pénale, ordonner l'interception, l'enregistrement et la transcription des correspondances émises par la voie des télécommunications à destination de lignes téléphoniques localisées à l'étranger dès lors que les interceptions, réalisées à partir de centres internationaux de transit situés en France, portent sur les appels émis depuis le territoire français; qu'en autorisant l'interception de la ligne téléphonique espagnole n° 00... susceptible d'être utilisée par Mario X... ainsi que l'enregistrement des appels envoyés-reçus sur le territoire national par cette ligne et leur transcription, ce qui incluait d'autres appels que ceux simplement émis depuis le territoire français, la chambre de l'instruction a violé les textes et le principe susvisés;

« alors, d'autre part, que pour décider que seules ont été transcrites les conversations émises en France à destination de la ligne écoutée, la chambre de l'instruction s'est bornée à relever que la réquisition à l'origine de ces écoutes était limitée aux "appels au départ du territoire national à destination de la ligne cellulaire espagnole"; qu'ainsi, en déduisant la conformité des conversations transcrites d'une réquisition qui était nécessairement antérieure et ne préjugait en rien de leur régularité, la chambre de l'instruction a privé sa décision de toute base légale;

« alors, enfin qu'en l'absence de toute indication sur les transcriptions des conversations téléphoniques, il n'était pas possible de déterminer si les conversations passées sur la ligne surveillée ont été émises ou reçues alors que seules les conversations émises depuis le territoire national à destination de la ligne espagnole devaient être enregistrées, de telle sorte qu'elles devaient être annulées ainsi que les actes dont elles étaient le support nécessaire »;

Attendu que le moyen, qui se borne à reprendre l'argumentation que, par une motivation exempte d'insuffisance comme de contradiction, la chambre de l'instruction a écarté à bon droit, ne saurait être accueilli;

Sur le troisième moyen de cassation, pris de la violation des articles 706-95, 100, 100-1 à 100-5, 171, 591 à 593 du Code de procédure pénale, défaut de motifs, manque de base légale;

« en ce que l'arrêt attaqué a refusé d'annuler les mesures d'enregistrement et de transcription de la ligne espagnole n° 00...;

« aux motifs que comme le prévoit l'article 100-4 du Code de procédure pénale, l'opération d'interception doit donner lieu à la rédaction d'un procès-verbal mentionnant la date et l'heure auxquelles elle a commencé et celles auxquelles elle s'est terminée; que chaque enregistrement doit ensuite donner lieu à l'établissement d'un procès-verbal qui précise également la date et l'heure de début et de fin de l'enregistrement, que par ailleurs, toute correspondance enregistrée est placée sous scellés; que les écoutes téléphoniques, autorisées le 28 juillet 2006 pour une durée de quinze jours par le juge des libertés et de la détention, se sont déroulées du 28 juillet au 4 août 2006 (tome 4 / D. 1898 à D. 1900); que ce magistrat a été avisé de leur mise en place le 31 juillet 2006 (tome 2 / D. 50); que le 4 août 2006, le procureur de la République l'a informé par écrit de ce que sept des écoutes qu'il avait autorisées pour une durée précisée dans l'avis, dont celles objet de la requête en annulation, avaient toutes été opérationnelles, de ce qu'elles avaient permis d'établir l'existence d'un trafic international de produits stupéfiants, et de ce qu'il requerrait l'ouverture d'une information (tome 23 / D. 12); que le rapport de synthèse des écoutes réalisées établi par les enquêteurs a été annexé au courrier (tome 2 / D. 13 à D. 14); que l'article 706-95 du Code de procédure pénale qui impose au procureur de la République d'informer sans délai le juge des libertés et de la détention des actes accomplis en exécution de son ordonnance d'autorisation ne visent que les diligences effectuées et non leur contenu, aucune disposition ne prévoyant expressément la transmission des pièces d'exécution à ce magistrat dont le pouvoir de contrôle porte non pas sur les modalités de transcription des interceptions mais sur la ligne concernée, la durée de l'opération, et son résultat, le cas échéant sur l'opportunité de son maintien; que le procureur de la République n'avait donc pas à transmettre au juge des libertés et de la détention les procès-verbaux d'écoute, soit les vingt-sept feuillets supportant les retranscriptions des conversations interceptées (D. 1902), le contrôle de leur régularité ressortant en l'espèce de la compétence de la chambre de l'instruction;

« alors qu'il résulte des dispositions de l'article 706-95 du Code de procédure pénale que le juge des libertés et de la détention qui a autorisé les opérations d'interception, d'enregistrement et de transcription de correspondances téléphoniques doit être informé, sans délai, par le procureur de la République des actes accomplis pour ces opérations; que

cette information est une formalité d'ordre public qui nécessite que le juge des libertés et de la détention soit informé sans délai de l'ensemble des mesures prises en application de l'autorisation qu'il a donnée sous peine de nullité; qu'il résulte, en l'espèce des propres constatations de l'arrêt que le juge des libertés et de la détention qui a autorisé les opérations d'interception n'a pas été destinataire des procès-verbaux des opérations d'interception, d'enregistrement et de transcription mais uniquement d'un compte rendu et d'un rapport de synthèse à l'issue des opérations; que, dès lors, en écartant la nullité des écoutes, la chambre de l'instruction a violé les textes précités »;

Attendu que le requérant a soutenu que les écoutes autorisées par le juge des libertés et de la détention, le 28 juillet 2006, devaient être annulées, ce magistrat n'ayant pas été destinataire des procès-verbaux d'interception;

Attendu que, pour rejeter cette argumentation, l'arrêt retient, notamment, que le procureur de la République a informé le juge des libertés et de la détention de la mise en place des écoutes, le 31 juillet 2006, puis, le 4 août 2006, de ce qu'elles avaient permis d'établir l'existence d'un trafic international de stupéfiants, enfin, de l'ouverture d'une information, le même jour; que les juges relèvent qu'en l'absence d'une disposition légale imposant la transmission des procès-verbaux d'exécution au juge des libertés et de la détention, les informations données à ce magistrat par le procureur de la République portent sur les diligences effectuées et non sur leur contenu;

Attendu qu'en prononçant ainsi, la chambre de l'instruction a justifié sa décision au regard de l'article 706-95 du Code de procédure pénale;

D'où il suit que le moyen n'est pas fondé;

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

REJETTE le pourvoi;

Ainsi fait et jugé par la Cour de cassation, chambre criminelle, et prononcé par le président le vingt-six mars deux mille huit;

En foi de quoi le présent arrêt a été signé par le président, le rapporteur et le greffier de chambre.



**Cour de cassation**  
**Chambre commerciale**  
**Audience publique du mardi 3 juin 2008**  
**N° de pourvoi : 07-17147 07-17196**  
Publié au bulletin **Cassation**

*CONVENTION EUROPÉENNE DES DROITS DE L'HOMME – Article 6  
§ 1 – Équité – Violation – Cas – Enregistrement d'une communication  
téléphonique à l'insu de l'auteur des propos tenus – Portée*

*L'enregistrement d'une communication téléphonique par une partie à l'insu de l'auteur des propos tenus constitue un procédé déloyal rendant irrecevable sa production à titre de preuve*

LA COUR DE CASSATION, CHAMBRE COMMERCIALE, a rendu l'arrêt suivant :

Sur le premier moyen, pris en sa première branche, du pourvoi formé par la société Sony et le premier moyen, pris en sa première branche, du pourvoi formé par la société Philips, réunis :

Vu l'article 6 § 1 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales;

Attendu que l'enregistrement d'une communication téléphonique réalisé par une partie à l'insu de l'auteur des propos tenus constitue un procédé déloyal rendant irrecevable sa production à titre de preuve;

Attendu, selon l'arrêt attaqué, que, saisi par la société Avantage – TVHA (la société Avantage) de pratiques qu'elle estimait anticoncurrentielles, mises en œuvre par des fournisseurs et des distributeurs de produits d'électronique grand public, le Conseil de la concurrence (le Conseil) a, par une décision n° 05-D-66 du 5 décembre 2005, dit établi que plusieurs sociétés dont les sociétés Philips France (la société Philips) et la société Sony France (la société Sony) ont enfreint les dispositions de l'article L. 420-1 du Code de commerce en mettant en œuvre, de novembre 1997 à fin 1998, une entente avec leurs distributeurs relative à l'application de prix conseillés sur un certain nombre de produits d'électronique grand public et a prononcé des sanctions pécuniaires de 16 millions d'euros à l'encontre de chacune d'elles;

Attendu que pour rejeter le recours formé par ces sociétés contre la décision du Conseil, l'arrêt retient qu'en l'absence de texte réglementant la production des preuves par les parties à l'occasion de procédures suivies devant lui sur le fondement des articles L. 420-1 et L. 420-2 du Code de commerce, c'est à bon droit que le Conseil, qui bénéficie d'une autonomie procédurale tant à l'égard du droit judiciaire privé national qu'à l'égard du droit communautaire, a retenu, en se fondant sur sa mission de protection de l'ordre public économique, sur le caractère représ-

sif de ces poursuites conduisant au prononcé de sanctions pécuniaires et sur l'efficacité qui en est attendue, que les enregistrements de communications téléphoniques, qui étaient produits par la partie saisissante et non par les enquêteurs ou le rapporteur, ne pouvaient être écartés au seul motif qu'ils avaient été obtenus de façon déloyale, qu'ils étaient recevables dès lors qu'ils avaient été soumis à la contradiction et qu'il lui appartenait seulement d'en apprécier la valeur probante ;

Attendu qu'en statuant ainsi, la cour d'appel a violé le texte susvisé ;

PAR CES MOTIFS, et sans qu'il y ait lieu de statuer sur les autres griefs :

CASSE ET ANNULE, dans toutes ses dispositions, l'arrêt rendu le 19 juin 2007, entre les parties, par la cour d'appel de Paris ; remet, en conséquence, la cause et les parties dans l'état où elles se trouvaient avant ledit arrêt et, pour être fait droit, les renvoie devant la cour d'appel de Paris, autrement composée ;

Condamne le ministre de l'Économie, des Finances et de l'Industrie aux dépens ;

Vu l'article 700 du Code de procédure civile, rejette les demandes ;

Dit que sur les diligences du procureur général près la Cour de cassation, le présent arrêt sera transmis pour être transcrit en marge ou à la suite de l'arrêt cassé ;

Ainsi fait et jugé par la Cour de cassation, chambre commerciale, financière et économique, et prononcé par le président en son audience publique du trois juin deux mille huit.

**Cour de cassation**  
**Chambre criminelle**  
**Audience publique du mardi 30 septembre 2008**  
**N° de pourvoi : 07-82249**  
Publié au bulletin **Rejet**

Cet arrêt est disponible de façon exhaustive sur le site de la cour de cassation. Il a par souci d'économie de moyens fait l'objet de coupes.

Résumé :

*Le délit d'atteinte à l'intimité de la vie privée est constitué, même en l'absence de retranscription des communications interceptées.*

*Le commandement de l'autorité légitime ne peut être invoqué lorsque l'ordre est manifestement illégal, en particulier il ne peut être retenu « en faveur d'un officier supérieur de la gendarmerie et de hauts fonctionnaires, dès lors que ne leur était imposée aucune obéissance inconditionnelle à des ordres manifestement illégaux ».*

*Le seul fait pour le directeur du GIC de ne pas s'être opposé à la sortie de documents retranscrivant des écoutes portant par elles-mêmes atteinte à l'intimité de la vie privée permet de retenir à son encontre ce même délit.*

*Est détachable de la fonction d'un agent public, même si elle n'est pas dépourvue de tout lien avec son service, la faute de cet agent qui, impliquant une intention de nuire ou présentant une gravité particulière, révèle un manquement volontaire et inexcusable à des obligations d'ordre professionnel et déontologique. Tel est le cas notamment des prévenus, hauts fonctionnaires ou hauts gradés de la gendarmerie ou de la police nationale qui, par la commission de faits illégaux relevant d'un système institutionnalisé et constitutifs de délits d'atteinte à l'intimité de la vie privée, « ont jeté le discrédit sur l'ensemble de la fonction publique civile et militaire en affaiblissant l'autorité de l'État dans l'opinion publique, méconnaissant ainsi l'intérêt général, au seul profit d'intérêts particuliers n'excluant nullement leurs propres intérêts de carrière ».*

LA COUR DE CASSATION, CHAMBRE CRIMINELLE, a rendu l'arrêt suivant :

Statuant sur les pourvois formés par :

- X... Christian,
- E... Pierre-Yves,
- Y... Gilles,
- Z... Louis,
- A... Pierre,
- B... Jean-Louis,
- C... Paul,
- D... Jacques, partie civile,

contre l'arrêt de la cour d'appel de PARIS, 11<sup>e</sup> chambre, en date du 13 mars 2007, qui a prononcé sur les intérêts civils dans la procédure suivie contre les six premiers des chefs d'atteintes à l'intimité de la vie privée, et qui a condamné le septième à six mois d'emprisonnement avec sursis et 5000 euros d'amende du chef de recel ;

La COUR, statuant après débats en l'audience publique du 2 septembre 2008

[...]

Attendu qu'il résulte de l'arrêt attaqué et des pièces de procédure qu'au cours de l'année 1992, à la suite d'articles de presse faisant apparaître le placement irrégulier sous écoutes téléphoniques d'un avocat et d'un journaliste, des informations judiciaires ont été ouvertes notamment des chefs d'atteintes à l'intimité de la vie privée; qu'il est apparu que, de 1983 à 1986, la « mission de coordination, d'information et d'action contre le terrorisme », autrement dénommée « la cellule élyséenne »,

composée de militaires de la gendarmerie, de fonctionnaires de la direction de la surveillance du territoire (DST) et de policiers des renseignements généraux en détachement, et dirigée par Christian X..., ancien membre du groupement d'intervention de la gendarmerie nationale (GIGN), conseiller technique du Président de la République, avait exercé, sur les instructions de Gilles Y..., directeur adjoint, puis directeur du cabinet du Président de la République, la surveillance habituelle d'une vingtaine de lignes téléphoniques et ainsi intercepté les correspondants de personnalités; qu'en outre, les expertises judiciaires de cinq disquettes informatiques déposées le 12 janvier 1995 par une personne non identifiée au tribunal de grande instance de Paris ont révélé qu'il avait été procédé au traitement automatisé d'informations nominatives concernant les personnes dont les lignes téléphoniques avaient été surveillées, ainsi que de leurs interlocuteurs;

Attendu que ces agissements ont entraîné le renvoi devant le tribunal correctionnel notamment des chefs d'atteintes à l'intimité de la vie privée, outre de Gilles Y... et de Christian X..., de Jean-Louis B..., officier général de gendarmerie détaché au cabinet militaire du Président de la République, de Pierre-Yves E..., commissaire de la DST mis à disposition de la présidence de la République, de Pierre A..., général de l'armée de terre responsable du Groupement Interministériel de Contrôle (GIC) et de Louis Z..., directeur de cabinet du Premier ministre entre 1984 et 1986 et signataire par délégation du Premier ministre des autorisations d'interceptions administratives de sécurité, ainsi que de Paul C..., ancien membre du GIGN, qui avait pris part de façon officieuse aux travaux de « la cellule élyséenne », ce dernier du chef de recel de fichiers informatiques contenant des données nominatives recueillies hors des cas prévus par la loi;

Attendu que le tribunal correctionnel a dit la prévention pour partie établie; qu'il a en outre déclaré irrecevables certaines des constitutions de partie civile et jugé que l'action civile, pour les faits retenus, relevait de la compétence de la juridiction administrative, en l'absence de fautes détachables du service; que les parties civiles qui avaient été déboutées de leur action ont interjeté appel du jugement, cette décision n'étant remise en cause sur l'action publique que sur les appels de Paul C... et du ministère public à l'égard de ce prévenu;

En cet état :

[...]

#### **Sur le délit d'atteinte à l'intimité de la vie privée (NDLR CNCIS),**

Attendu que, pour dire que les agissements reprochés aux prévenus caractérisent le délit d'atteinte à l'intimité de la vie privée prévu, à la date des faits, par l'article 368 du Code pénal devenu l'article 226-1 du même Code, l'arrêt retient que, le 12 janvier 1995, il a été remis au juge d'instruction cinq disquettes provenant de la "cellule élyséenne"

et contenant vingt-six fichiers créés grâce à l'emploi d'un logiciel mis à la disposition de cet organisme, parmi lesquels se trouvaient les listes des correspondants des personnes écoutées et plus de trois mille fiches de synthèses de conversations téléphoniques irrégulièrement captées en 1985 et 1986; que les juges ajoutent que, compte tenu des résultats des expertises et de l'examen des documents ou bandes magnétiques saisis dans un garage mis à la disposition de Christian X..., la matérialité et le contenu des fichiers extraits des disquettes ne peuvent utilement être contestés par les prévenus, lesquels n'ont d'ailleurs exercé aucune voie de recours contre la décision du tribunal retenant, en fonction des mêmes éléments de preuve, leur culpabilité à l'égard de certaines parties civiles; que la cour d'appel énonce enfin que les interceptions, pratiquées hors d'un cadre légal et sans respecter les recommandations d'un rapport de l'autorité judiciaire, sont avérées et que, même si quelques-unes d'entre elles n'ont pas fait l'objet d'une transcription, elles caractérisent en tous ses éléments, y compris l'élément intentionnel, le délit d'atteinte à l'intimité de la vie privée, dès lors que les branchements clandestins et illégaux sur les lignes téléphoniques du domicile ou du local professionnel des parties civiles ont, par leur conception, leur objet et leur durée, nécessairement conduit leurs auteurs à pénétrer dans l'intimité de la vie privée des personnes mises sous écoutes et de leurs interlocuteurs;

Attendu qu'en cet état, et abstraction faite du motif surabondant, mais non déterminant, relatif à l'application de dispositions conventionnelles pour la détermination des éléments constitutifs de l'infraction retenue, les juges du second degré, qui ont répondu aux chefs péremptaires des conclusions dont ils étaient saisis, ont fait l'exacte application des dispositions de l'article 368 de l'ancien Code pénal dans sa rédaction issue de la loi du 17 juillet 1970, et ainsi justifié leur décision;

D'où il suit que les moyens doivent être écartés;

[...]

#### **Sur l'irresponsabilité tirée du commandement de l'autorité légitime (NDLR CNCIS)**

[...]

Attendu que, pour refuser aux prévenus le bénéfice du fait justificatif prévu par l'article 327 de l'ancien Code pénal devenu l'article 122-4 du même Code, relatif au commandement de l'autorité légitime, l'arrêt relève qu'à l'époque des faits, aucune loi ne prévoyait les interceptions administratives, qui étaient mises en œuvre selon la décision n° 1 E du Premier ministre en date du 28 mars 1960 complétée par les recommandations d'un rapport de l'autorité judiciaire; que l'arrêt observe également que le dépassement de son champ de compétence par « la cellule élyséenne » a entraîné une large confusion entre les missions de lutte contre le terrorisme, la sécurité du Président de la République ainsi que de ses proches et la protection de la vie privée de ce dernier, et qu'à le

supposer donné par le chef de l'État, l'ordre de procéder à des écoutes pour protéger sa vie privée ne pouvait légitimer cet acte, dès lors qu'il émanait d'une autorité ne disposant pas du pouvoir de le faire; que les juges ajoutent que les écoutes téléphoniques en cause ont été pratiquées de façon illégitime, sans respecter la procédure administrative mise en place ni les directives des Premiers ministres qui avaient interdit, sauf motifs particuliers sur lesquels l'attention devait être alertée, l'écoute d'avocats et de journalistes; que les juges énoncent enfin que le commandement de l'autorité légitime ne peut être retenu en faveur d'un officier supérieur de la gendarmerie et de hauts fonctionnaires, dès lors que ne leur était imposée aucune obéissance inconditionnelle à des ordres manifestement illégaux;

Attendu qu'en l'état de ces motifs, qui caractérisent des comportements faisant obstacle à l'application du fait justificatif invoqué, la cour d'appel a justifié sa décision;

D'où il suit que les moyens doivent être écartés;

#### **Sur la participation matérielle du chef du GIC au délit d'atteinte à l'intimité de la vie privée (NDLR CNCIS)**

Attendu que, pour dire Pierre A... coupable de faits caractérisant le délit d'atteinte à l'intimité de la vie privée, l'arrêt énonce qu'en sa qualité de chef du GIC, organisme placé sous le contrôle du Premier ministre, le prévenu était chargé de la mise en place des interceptions demandées par le ministre de la Défense, après réception de l'aval du directeur de cabinet du Premier ministre, ainsi que de leur transcription et de leur diffusion; que les juges ajoutent que ledit prévenu, connaissant le fondement juridique fragile des interceptions demandées par « la cellule élyséenne » qui lui étaient signalées, n'a pas estimé devoir attirer l'attention du cabinet du Premier ministre et ne s'est pas opposé à la sortie, hors de son service, d'un nombre significatif d'interceptions dont la « cellule » opérait elle-même irrégulièrement la transcription; que la cour d'appel déduit de l'ensemble de ces éléments que Pierre A... a pris part, délibérément, aux écoutes illégales;

Attendu qu'en l'état de ces motifs, qui répondent aux chefs péremptoires des conclusions dont ils étaient saisis, les juges du second degré ont justifié leur décision;

Qu'il s'ensuit que le moyen ne peut être admis;

#### **Sur le caractère détachable des fonctions de la faute commise (NDLR CNCIS)**

Attendu qu'après avoir relevé qu'est détachable de la fonction d'un agent public, même si elle n'est pas dépourvue de tout lien avec son service, la faute de cet agent qui, impliquant une intention de nuire ou présentant une gravité particulière, révèle un manquement volontaire et inexcusable à des obligations d'ordre professionnel et déontologique,

l'arrêt, pour statuer sur les demandes de réparations des parties civiles, retient que tel est le cas des prévenus, hauts fonctionnaires ou hauts gradés de la gendarmerie ou de la police nationale qui, par la commission de faits illégaux relevant d'un système institutionnalisé et constitutifs de délits d'atteinte à l'intimité de la vie privée, ont jeté le discrédit sur l'ensemble de la fonction publique civile et militaire en affaiblissant l'autorité de l'État dans l'opinion publique, méconnaissant ainsi l'intérêt général, au seul profit d'intérêts particuliers n'excluant nullement leurs propres intérêts de carrière ;

Attendu qu'en se déterminant ainsi, la cour d'appel, qui a fait l'exacte application des dispositions et principes invoqués, a justifié sa décision ;

D'où il suit que les moyens ne sauraient être accueillis ;

[...]

III – Sur les autres pourvois :

Les REJETTE ;

[...]

Ainsi fait et jugé par la Cour de cassation, chambre criminelle, et, prononcé par le président le trente septembre deux mille huit ;

En foi de quoi le présent arrêt a été signé par le président, le rapporteur et le greffier de chambre.

# 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
Relations extérieures.....	12
Chapitre II	
<b>Le contrôle des interceptions de sécurité (loi n° 91-646 du 10 juillet 1991)</b> .....	13
Le contrôle des autorisations .....	13
Le contrôle de l'exécution.....	23
Le contrôle du matériel .....	26
Chapitre III	
<b>Le contrôle des opérations de communication des données techniques (loi n° 2006-64 du 23 janvier 2006)</b> .....	29
Présentation du dispositif .....	29
Éléments d'ordre statistique.....	30
Étendue et modalités du contrôle exercé par la CNCIS .....	31



Deuxième partie

<b>JURISPRUDENCE DE LA COMMISSION</b> .....	35
La qualité de la motivation des demandes d'interception .....	37
Sécurité nationale .....	40
Sauvegarde des éléments essentiels du potentiel scientifique et économique de la Nation.....	42
Prévention du terrorisme .....	45
Prévention de la criminalité et de la délinquance organisées .....	47

Troisième partie

<b>ÉTUDES ET DOCUMENTS</b> .....	51
----------------------------------	----

Chapitre I

<b>Présentation ordonnée des textes relatifs aux missions de la Commission</b> .....	53
Première mission : les interceptions .....	53
Deuxième mission : les opérations de communications de données techniques (loi 2006-64 du 23 janvier 2006) .....	68
Troisième mission : le contrôle du matériel .....	72

Chapitre II

<b>Actualité législative et réglementaire</b> .....	81
Loi n° 2008-1245 du 1 <sup>er</sup> décembre 2008 visant à prolonger l'application des articles 3, 6 et 9 de la 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.....	81
Décret n° 2008-609 du 27 juin 2008 relatif aux missions et à l'organisation de la direction centrale du renseignement intérieur .....	81

Chapitre III

<b>Interceptions de sécurité et secret-défense</b> .....	85
--	----

Chapitre IV

<b>Jurisprudence des cours et tribunaux</b> .....	87
Jurisprudence européenne.....	87
Jurisprudence française.....	89