Commission nationale de contrôle des interceptions de sécurité

18e rapport d'activité

Année 2009

La documentation Française

Sommaire

Avant-propos

Pour la Commission, le bilan de l'année 2009 se place sous le double signe de la continuité dans la transition, dans un cadre politique et administratif pratiquement inchangé.

Les indicateurs « quantitatifs » sont comparables à ceux de 2008 dès lors qu'on prend en compte la réduction de moitié du nombre des « urgences », conséquence mécanique du passage à la « cible ». Le total des interceptions de sécurité réalisées a ainsi atteint le chiffre de 5029 contre 5906 en 2008. La proportion entre demandes initiales et renouvellements est modifiée en conséquence : 1916 renouvellements, correspondant à des cibles potentiellement dangereuses qu'il faut suivre au-delà de la période initiale d'interception. Les motifs restent statistiquement stables : deux tiers pour la criminalité organisée, un peu moins d'un quart pour le terrorisme et un peu moins du cinquième pour la sécurité nationale.

En revanche, en ce qui concerne la pratique du contrôle, il convient de procéder à une lecture différente du thème de la continuité. Ici continuité ne signifie pas stabilité, mais accroissement de l'intensité de contrôle, dans la ligne déjà amorcée en 2008 par rapport à 2007.

La pratique du suivi des « productions » a connu de nouveaux développements : 326 dossiers ont été ainsi « suivis » en 2009 contre 172 en 2008. Ceci a induit un nombre plus élevé d'observations et de recommandations de cessation de l'interception en cours d'exploitation ou d'avertissement adressés au Premier ministre, sans compter les « préconisations » d'interceptions directement adressées aux services et suivies par ceux-ci.

Enfin, toujours dans la même ligne, on notera l'accroissement du contrôle dans le domaine de l'article 6 de la loi de 2006.

La transition a donc concerné, comme déjà indiqué le passage à la cible : ce passage, demandé depuis de longues années par les services, et accepté fin 2008 par la Commission pour des raisons notamment dues à l'évolution technologique a induit la mise en place de nouveaux formulaires, mis au point avec l'aide précieuse du GIC, et qui ont permis un dialogue renouvelé avec les services.

L'année 2009 aura vu le départ quasi simultané de l'Inspecteur Général François JASPART, « personnalité qualifiée » au titre de l'article 6 de la loi de 2006, et du Président Jean Louis DEWOST dont le mandat de six ans est venu à expiration en septembre 2009.

Je ne peux que rendre un grand hommage à mon prédécesseur qui, durant son mandat, a rendu possible l'adaptation à droit constant des travaux et missions de la Commission face aux nouvelles technologies en matière de communications électroniques. On lui doit aussi à la fois la préparation et la mise en place du dispositif résultant de la loi du 23 janvier 2006. Il aura enfin accompli une œuvre réformatrice en ce qui concerne les techniques de contrôle développées par la Commission.

Hervé PELLETIER
Président de la Commission

Première partie

RAPPORT D'ACTIVITÉ

Chapitre I

Organisation et fonctionnement de la Commission

Composition de la Commission

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

Membres de la Commission :

• Président jusqu'au 30 septembre 2009 : 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)

• Hervé PELLETIER, président de chambre à la Cour de Cassation, nommé pour une durée de six ans par le Président de la République (décret du 3 octobre 2009, publié au *Journal officiel* le 4 octobre 2009)

• Membre parlementaire – Sénat : Hubert HAENEL, sénateur (UMP) du Haut-Rhin, désigné le 15 octobre 2008 par le Président du Sénat.

• Membre parlementaire – Assemblée nationale : Daniel VAILLANT, député (PS) de Paris, désigné le 1er 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-José MASSET.

Christophe GERMIN conduit le véhicule de la Commission.

Rappel des compositions successives de la Commission

Présidents :
• Paul BOUCHET, conseiller d'État, 1er octobre 1991
• Dieudonné MANDELKERN, président de section au Conseil d'État, 1er octobre 1997
• Jean-Louis DEWOST, président de section au Conseil d'État, 1er octobre 2003
• Hervé PELLETIER, président de chambre à la Cour de Cassation, 3 octobre 2009

Représentants de l'Assemblée nationale :
• François MASSOT, député des Alpes-de-Haute-Provence, 19 juillet 1991
• Bernard DEROSIER, député du Nord, 24 mai 1993
• Jean-Michel BOUCHERON, député d'Ille-et-Vilaine, 3 juillet 1997
• Henri CUQ, député des Yvelines, 4 juillet 2002
• Bernard DEROSIER, député du Nord, 20 mars 2003
• Daniel VAILLANT, député de Paris, 1er août 2007

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 nº 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 nº 2006-64 du 23 janvier 2006.

Conformément à l'article 1er de son règlement intérieur, « la Commission se réunit à intervalles réguliers à l'initiative de son président ; elle peut également être réunie à la demande d'un de ses membres ». Entre 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 nº 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 nº 97-757 du 10 juillet 1997 qui, sous la présidence du directeur général de l'agence nationale de la sécurité des systèmes d'information, 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 2009 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 308 – Protection des droits et libertés.

Afin de respecter l'indépendance budgétaire de notre autorité, celle-ci a été dotée d'un budget opérationnel de programme (BOP), référencé 308AIC. Les crédits alloués en 2009 se sont élevés à 568 257 euros dont 486 344 euros pour les dépenses du titre II (dépenses de personnel) et à 81 913 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 2009 d'importants travaux de rationalisation financière au sein desquels on peut, à titre d'exemple, citer la mutualisation des coûts d'entretien et de réparation automobile avec les services du Premier ministre.

Relations extérieures

Au mois de décembre 2009, et à la demande de Monsieur l'Ambassadeur de France en Bulgarie relayant le souhait des autorités bulgares de pouvoir bénéficier du concours de la France dans leurs travaux d'élaboration d'une nouvelle législation en matière d'interception des communications électroniques, le Délégué général a effectué une mission d'information au profit de ces autorités reposant sur l'exposé du « modèle français » à partir de la loi du 10 juillet 1991 à la faveur de regards croisés sur le « modèle bulgare » et notamment sur la loi du 21 octobre 1997 portant sur les moyens spéciaux de renseignements. Durant ces trois journées de travaux, le Délégué général a ainsi pu échanger avec le Vice ministre de l'intérieur, la Présidente de la Commission d'État pour la sécurité de l'information, la Vice ministre de la justice et la Commission parlementaire de la sécurité intérieure et de l'ordre public.

Ces travaux devraient, selon le vœu des autorités bulgares, se poursuivre en 2010.

Chapitre II

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 demandes d'interceptions de sécurité. Elle se traduit par un contrôle systématique et exhaustif de l'ensemble de ces 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 nº 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, 3e 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	2009*
Ministère de la Défense	232	330	400	450	285
Ministère de l'Intérieur	928	1 190	1 190	1 290	1 455
Ministère du Budget	20	20	80	100	100
Total	**1 180**	**1 540**	**1 670**	**1 840**	**1 840**

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

L'année 2009 a été marquée par la mise en œuvre au 1er janvier de l'interprétation par la Commission de ce contingent comme se référant à un nombre maximum de « cibles » et non plus de « lignes ». Outre la diminution importante du nombre « d'urgences absolues » que ce passage a induit, cette référence à la « cible » doit permettre de ne pas envisager une augmentation de ce contingent 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, en 2008 et à nouveau en 2009 pour tendre, à partir des modèles les plus complets, à une uniformisation de la présentation gage d'une meilleure égalité d'appréciation et de permettre également de potentialiser encore le contrôle de la Commission dans le cadre du passage à « l'autorisation par cible ». 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 tra-

duire *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[1], par 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 2008-2009

5 117 interceptions de sécurité ont été sollicitées en 2009 (3 176 interceptions initiales et 1 941 renouvellements).

S'agissant des interceptions initiales, 497 de ces 3 176 demandes ont été présentées selon la procédure dite d'urgence absolue (1 095 en 2008) soit 18,90 % de ces demandes (25 % en 2008). Cette chute importante du nombre des urgences absolues résulte du « passage à l'autorisation par cible » qui a induit la suppression des urgences « techniques » qui représentaient, en 2008, 56,70 % des urgences.

Ces urgences dites « techniques » étaient initialement destinées à pallier la possible interruption de la surveillance résultant d'un changement de ligne ou de vecteur de communication par une cible ou de son utilisation de plusieurs lignes en concomitance.

L'objectif d'un traitement par la Commission de ce type de demande dans un délai inférieur à une heure a, cette année encore, été respecté. La réalisation de cet objectif nécessite, dans le cadre de « l'avis à priori » donné par la Commission, la mise en œuvre d'une permanence comparable à celle qui est assurée par chaque Parquet près les tribunaux de grande instance.

Au final, si l'on impute à ce chiffre global les 88 avis négatifs donnés par la Commission lors des demandes initiales et des demandes de renouvellement, tous suivis à une seule exception par le Premier ministre, ce sont donc 5 029 interceptions de sécurité qui ont effectivement été pratiquées au cours de l'année 2009 (5 906 en 2008).

---

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 récidive d'une infraction criminelle déjà commise, délai *ad hoc* calé sur un événement prévu à date fixe, etc.

Pour ce qui concerne les motifs au stade des demandes initiales, la prévention de la criminalité et délinquance organisées reste le premier motif des demandes initiales avec 59,20 % (59 % en 2008), suivie de la prévention du terrorisme avec 22,50 % (26,50 % en 2008) et la sécurité nationale 17,50 % (13 % en 2008).

Concernant les renouvellements, on note que la sécurité nationale occupe la première place avec 41,60 % (47 % en 2008), suivie de la prévention du terrorisme 38,80 % (38 % en 2008) et de la criminalité organisée 18 % (14 % en 2008). Ces pourcentages de renouvellement rendent de fait compte du travail des services au cœur de motifs qui supposent une inscription de l'investigation dans la durée.

Au total, demandes initiales et renouvellements confondus, c'est encore une fois la prévention de la criminalité et de la délinquance organisées qui se détache nettement avec 43,50 % (47 % en 2008) suivie de la prévention du terrorisme 28,70 % (29,50 % en 2008) et la sécurité nationale 26,70 % (22 % en 2008). Ces trois motifs représentent quasiment 99 % du total des demandes.

• Observations

La Commission a poursuivi sa démarche de dialogue avec les services demandeurs. Celle-ci s'est traduite par une nette augmentation des réunions bilatérales avec ces mêmes services. Elle s'est également matérialisée, au stade de l'examen de leurs demandes, par une logique d'avis moins binaire (avis favorable/défavorable). De fait, le nombre d'observations a encore crû, passant de 1 239 en 2008 à 1 691 en 2009 dont 80 demandes de renseignements complémentaires et 384 limitations de la durée d'interception sollicitée. Les avis défavorables, comptabilisés dans les observations, sont en hausse : 88 (63 concernant les demandes initiales et 25 les demandes de renouvellement) tous suivis à une seule exception par le Premier ministre. À ce chiffre des avis défavorables « bruts », il convient d'ajouter deux techniques d'observation déjà répertoriées dans le rapport d'activité 2008 qui peuvent s'apparenter à « l'avis négatif » :
– la recommandation adressée au Premier ministre visant à l'interruption de l'interception en cours d'exploitation qui résulte de l'examen exhaustif des « productions » (transcriptions) opérées à partir d'une interception. Il y a été fait recours à 19 reprises en 2009 (12 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 les services utilisateurs à « abandonner » 21 interceptions en 2009 (28 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 pour l'année 2009 à 128.

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'assurer à la fois de la bonne adéquation de la demande au motif légal invoqué et de l'intérêt réel présenté par l'interception au regard des critères de proportionnalité et de subsidiarité. Ce « contrôle continu » 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 326 interceptions en 2009 (172 en 2008) ont-elles été examinées par la Commission.

La pratique de la « recommandation d'avertissement » décrite dans le rapport 2008 a également été poursuivie : il s'agit d'une lettre annonçant au Premier ministre qu'une recommandation d'interruption de l'écoute pourrait lui être envoyée à bref délai si l'incertitude sur l'adéquation entre le motif invoqué et la réalité des propos échangés devait se poursuivre. 13 de ces recommandations ont été ainsi adressées au Premier ministre au cours de l'année 2009.

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 5 029 interceptions accordées en 2009 contre 5 906 en 2008, 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.

Les présentes données chiffrées reflètent à partir de 2009 le passage à « l'autorisation par cible » réalisé par la Commission.

Tableaux annexes

Les demandes initiales d'interception

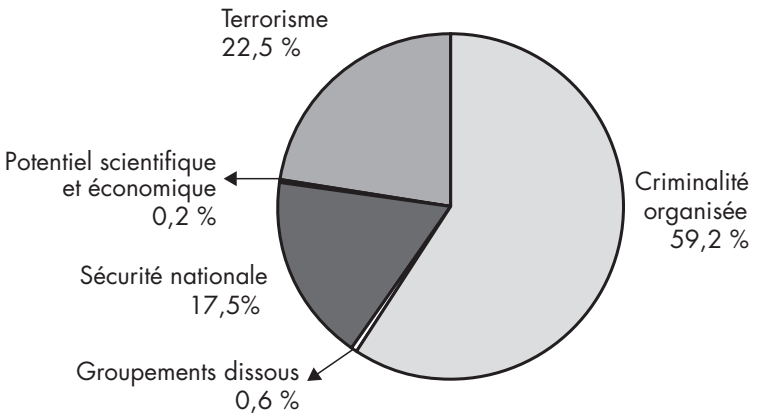
État des demandes initiales d'interception (2008 et 2009)

	Demandes initiales		Dont urgence absolue		Accordées	
	2008	2009	2008	2009	2008	2009
Totaux	4330	3176	1095	497	4311	3113

Demandes initiales

Répartition des motifs

2009

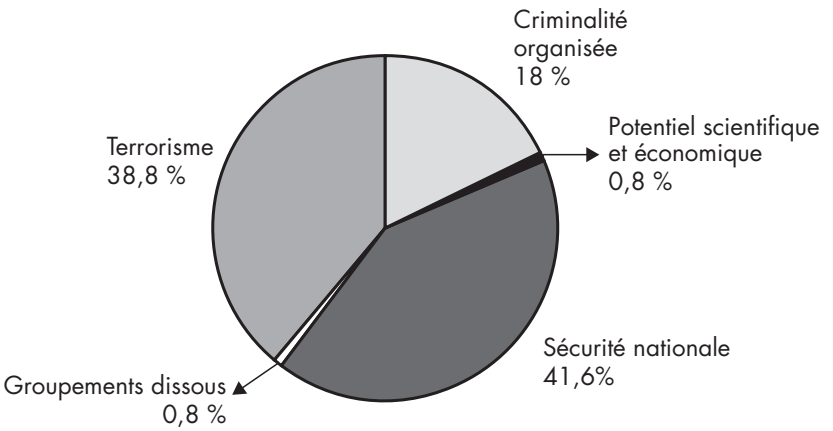


Les renouvellements d'interception

Répartition des motifs des renouvellements accordés en 2009

Sécurité nationale	Potentiel scientifique et économique	Terrorisme	Criminalité organisée	Groupements dissous	Total « demandés »	Total « accordés »
798	15	743	344	16	1941	1916

2009

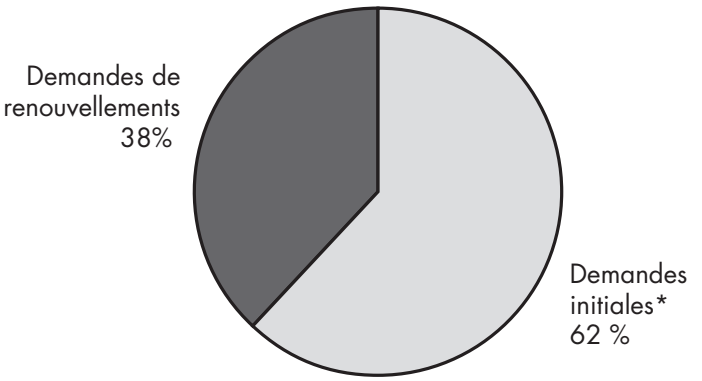


Activité globale : demandes initiales et renouvellements

Répartition des demandes entre interceptions et renouvellements d'interceptions

Demandes initiales circuit normal		Demandes initiales en urgence absolue		Demandes de renouvellements	
2008	**2009**	**2008**	**2009**	**2008**	**2009**
3235	2616	1095	497	1605	1916

2009



* Rappel : 18,9 % des demandes initiales sont constituées par des demandes présentées en « urgence absolue ».

Demandes d'interceptions : tableau récapitulatif global sur cinq ans

	2005	2006	2007	2008	2008
Demandes initiales d'interceptions	4144	4203	4215	4330	3176
Dont « urgence absolue »	854	714	964	1095	497
Demandes de renouvellements	1738	1825	1850	1605	1941
Total	**5882**	**6028**	**6065**	**5935**	**5117**

Répartition entre interceptions et renouvellements accordés

Interceptions accordées en 2009

Interceptions initiales	Renouvellements	Total
3113	1916	5029

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 cet article 12 n'édicte pas de délai, le GIC à la faveur d'une instruction permanente a, conformément aux prescriptions de l'IG 1 300/SGDN/SSD du 25 août 2003, imposé aux services destinataires finaux des productions, d'attester auprès de lui de la destruction effective de ces dernières dès lors que leur conservation ne présentait plus d'utilité pour l'exécution de la mission poursuivie.

Le contrôle du GIC

Service du Premier ministre, consacré comme tel après 31 années d'existence par le décret n° 2002-497 du 12 avril 2002 (CNCIS, 11e rapport 2002, p. 50) et actuellement dirigé par un officier général, le GIC est l'élément clef du dispositif des interceptions de sécurité. Il en assure la centralisation conformément à l'article 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, dix visites de centres d'exploitation 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, 42 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 télépho-

niques 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 ; ils ont 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] et reprise à l'article 41 de cette même loi, telle que modifiée par la loi du 6 août 2004 peut sembler insatisfaisante mais il est difficile, notamment au regard des prescriptions de l'article 26 de la loi du 10 juillet 1991 modifiée par la loi du 9 juillet 2004, d'aller plus loin dans la transparence. En effet, à l'occasion de son contrôle, la Commission peut découvrir les situations suivantes :
– existence d'une interception ordonnée par l'autorité judiciaire ;
– existence d'une interception de sécurité décidée et exécutée dans le respect des dispositions légales ;
– existence d'une interception de sécurité autorisée en violation de la loi ;
– existence d'une interception "sauvage", pratiquée en violation de l'article 1er 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 no 2088 de François MASSOT, 6 juin 1991).

Faut-il en conclure que toute requête est inutile ? Non, car même si le secret-défense interdit toute révélation sur l'existence ou l'inexistence d'une interception de sécurité, la CNCIS dispose de deux moyens d'action lorsqu'elle constate une anomalie :
– le pouvoir d'adresser au Premier ministre une recommandation tendant à faire interrompre une interception qui s'avérerait mal fondée ;
– le pouvoir, qui est aussi un devoir, de dénonciation à l'autorité judiciaire de toute infraction à la loi de 1991 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 2009, la CNCIS n'a pas eu à user des dispositions du 2e 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. Ces autorisations interviennent après avis d'une Commission consultative à laquelle participe la CNCIS. La structure de cette Commission a été modifiée à la faveur de 2 décrets publiés durant l'année 2009. Ainsi, le décret 2009-834 du 7 juillet 2009 puis le décret 2009-1657 du 24 décembre 2009 ont confié la présidence de cette Commission au Directeur général de l'agence nationale de la sécurité des systèmes d'information, lui-même rattaché au Secrétaire général de la Défense et de la sécurité nationale. Cette mutation structurelle n'a en revanche emporté aucune modification dans l'économie juridique du dispositif existant.

Le 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).

Si les règles de commercialisation ont été allégées par rapport au dispositif réglementaire antérieur à 2004, cette facilitation de l'accès au

marché n'a pas induit une inflexion dans la qualification du caractère « sensible » de ce type de matériel par les pouvoirs publics.

Ainsi, le décret 1739 du 30 décembre 2005 réglementant les relations financières avec l'étranger et portant application de l'article L. 151-3 du Code monétaire et financier (présenté en doctrine comme aménageant le contrôle des investissements étrangers dans les secteurs stratégiques en France – *Recueil* Dalloz 2006, p. 218) soumet au principe de l'autorisation préalable l'investissement d'un État (intra ou 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 2009. Sa composition est la suivante :
– le directeur de l'agence nationale de sécurité des systèmes d'information 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 2009, la Commission a rendu 588 décisions ventilées comme suit :
– 379 décisions d'autorisation initiale (266 concernant la commercialisation, 113 l'acquisition d'équipements soumis à autorisation) ;
– 41 décisions de renouvellement d'autorisation ;
– 74 décisions d'ajournement ;
– 4 décision de refus ou de retrait ;
– 53 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.

Chapitre III

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

Concernant le contrôle des opérations de communication des données techniques, 2009 aura constitué au-delà de la deuxième année « pleine » d'exercice de ce contrôle, une année de transition importante.

2009 aura en effet vu l'inspecteur général François JASPART quitter ses fonctions au terme du mandat légal de 3 ans qui lui avait été confié par la Commission le 26 décembre 2006. Il a été remplacé en qualité de « personnalité qualifiée » par le contrôleur général Jean ESPITALLIER à la faveur d'une décision de la Commission du 5 novembre 2009 publiée au journal officiel du 26 novembre 2009.

Que cette partie du rapport d'activité soit l'occasion de remercier publiquement François JASPART pour la qualité du « climat » de confiance qu'il a su instaurer avec la Commission, pour son incomparable travail de défricheur et de bâtisseur au cœur d'une matière où il a su avec patience et clairvoyance mettre en place des procédures, faire accepter un alignement de sa jurisprudence sur celle de la Commission et développer avec tous les acteurs de ce dispositif une démarche de collaboration constructive dans le respect des contraintes respectives de ces mêmes acteurs mais plus encore dans l'unique objectif de servir le vœu du législateur.

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 a vu le jour dans les faits le 2 mai 2007, et le présent rapport d'activité correspond à l'analyse de 2 années pleines d'utilisation de ce dispositif.

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 no 2008-1245 du 1er décembre 2008.

Présentation du dispositif

L'article 6 de la loi no 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'hyperterrorisme, 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 ». La Commission a eu recours à ce dispositif une seule fois en 2009.

Éléments d'ordre statistique

Pour l'année 2009, l'activité a été la suivante :
– 43 559 demandes présentées à la personnalité qualifiée ;
– 39 070 demandes validées ;
– 30 demandes refusées ;
– 4 459 demandes renvoyées au service demandeur pour renseignements complémentaires.

Pour mémoire, au titre de l'année 2008, l'activité avait 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.

En rythme annuel on peut, d'ores et déjà, observer que l'activité 2009 aura été un peu plus soutenue que l'année 2008. La baisse sensible du nombre de demandes refusées prend sa source dans plusieurs facteurs conjugués : d'abord une meilleure « maîtrise » par les services demandeurs des critères jurisprudentiels alignés par la Personnalité qualifiée sur ceux que la Commission applique pour le motif « prévention du terrorisme », ensuite une nette progression de la technique du bilatéral entre l'équipe de la « personnalité qualifiée » et les services demandeurs ; enfin le recours à une forme de « 3e voie », entre avis favorable ou rejet, comparable à celle que développe depuis plusieurs années la Commission pour les interceptions de sécurité et qui se traduit ici par la hausse du nombre des « demandes renvoyées pour renseignements complémentaires ».

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 2009, ce ne sont donc pas 43 559 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 en 2009 révèle que :
– 76 % concernent de simples demandes d'identification d'abonnés, mesures par essence moins attentatoires que les demandes portant sur le trafic observé sur une ligne, qui ont représenté 23 % des demandes traitées;
– une part résiduelle (1 %) 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 2009, conformément aux prescriptions de l'article 6 de la loi du 23 janvier 2006, la « personnalité qualifiée » a soumis son troisième rapport d'activité au président de la Commission, venant ainsi rendre compte de l'exercice des missions de contrôle qui lui ont été confiées par cette même loi.

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).

Le nombre de refus a significativement chuté (-67,7 % par rapport à 2008).

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 instaurant en 2009 un outil de plus au sein de ce « contrôle gradué » : la Commission a en effet, pour une quinzaine de dossiers, exercé, via la « personnalité qualifiée », un « droit de suite » en priant le service demandeur de bien vouloir lui préciser les suites données à cette demande en terme d'investigations. Par un rapide parallélisme, on peut rapprocher la mise en place de ce « droit de suite » au sein du dispositif de l'article 6 de la mise en œuvre du « contrôle des productions » pour ce qui concerne les interceptions de sécurité.

• 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 une recommandation écrite au ministre de l'Intérieur telles que prévues à l'article L. 34-1-1, 5e alinéa du Code des postes et communications électroniques, cette recommandation visait à rappeler que chacune des demandes formulées sur le fondement de l'article 6 de la loi du 23 janvier 2006 devait pouvoir être examinée de manière autonome, sans que l'autorité de contrôle (« personnalité qualifiée » dans son contrôle à priori ou la CNCIS dans son contrôle à posteriori) ait à rechercher l'existence d'un contexte ou d'autres éléments justifiant le bien fondé de la demande.

Deuxième partie

JURISPRUDENCE DE LA COMMISSION

Après 18 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 sur des demandes présentées sous la forme de « l'urgence absolue » déjà décrite.

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

Quelques lignes ne sauraient en effet suffire. 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. Elles privent également la Commission du contrôle sur l'articulation juridique entre des éléments factuels relevant du comportement de la cible et le motif légal d'interception invoqué par le service. Dans 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.

Ainsi une demande trop éloignée d'une implication directe et personnelle de la cible dans des faits participant du motif invoqué encourt la censure de la Commission. L'exemple volontairement imprécis tiré d'une demande où la démonstration de cette implication ne reposait que sur un « relationnel » avec d'autres individus peut être cité ici.

Une motivation pertinente

L'examen de cette pertinence porte sur 3 points :
– la motivation doit être exclusivement tournée vers la vocation préventive voulue par le législateur de 1991 pour les interceptions de sécurité. Outil de renseignement, ces mêmes interceptions ne peuvent être utilisées pour l'élucidation de faits passés sans préjudice de leur possible qualification pénale ;
– corrélativement, la motivation doit exclusivement se référer à des investigations participant de l'activité de renseignement et en aucun cas pouvoir générer un « risque d'interférence » avec une action judiciaire déjà déclenchée ;
– enfin, les soupçons qui pèsent sur la cible doivent nécessairement être en relation directe avec le motif. Ainsi un comportement dont la description reste floue, vague, imprécise et non « rattachable » au travail d'articulation juridique déjà décrit prive la demande de toute pertinence.

Tel a été, par exemple, le cas cette année d'une demande portant sur une cible non identifiée, suspectée « d'activités diverses » déployées sur « l'ensemble du territoire européen ».

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 pu, en revanche, soulever 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 affichée avec l'ordre établi a pu être « pimentée » par des références à des « actions passées » ou par l'utilisation de formules équivoques telles que « troubles de voie publique envisagés... » pour colorer une manifestation annoncée qui relève plus 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.

* * *

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 ».

Pour mémoire, on rappellera que l'article 8, § 2 de la Convention européenne des droits de l'homme dispose : « Il ne peut y avoir ingé-

rence 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.

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

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

Rapidement (rapport 1994, p. 17 et suiv.), 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 au bénéfice de ce raisonnement 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[1], 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"[2] » ; « [...] il est nécessaire que l'État dispose de moyens d'information et d'action adaptés aux **menaces** résultant de l'internationalisation des activités économiques[3] ».

« 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[4] ».

---

1) Assemblée nationale, 2e 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 no 2088, p. 29.
4) A. Vitu, articles 410-1 sqq, *Jurisclasseur pénal.*

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

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

Cette fourniture peut être le fait d'auteurs divers (ingénieurs, agents de renseignement de pays tiers, « honorables correspondants », officines « spécialisées » dans l'espionnage économique) et être destinée non seulement à des services de renseignements de pays tiers (« puissances étrangères ») mais également à des entreprises [1] 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.

---

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.

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 donc à des infractions précises.

La Jurisprudence de la Commission pour ce qui concerne ce motif s'efforce à une synthèse :
– du dispositif normatif pénal ainsi décrit ;
– du postulat originel de 1991 reposant sur l'aspect préventif et non proactif à l'instar d'une partie de la doctrine née de l'intelligence économique ;
– de la nécessaire protection du « noyau dur » de notre patrimoine scientifique et économique ;
– de la toute aussi nécessaire préservation de la « vie des affaires », elle aussi protégée juridiquement dans une zone européenne où le libre échange représente une valeur constitutive.

Ainsi, la Commission a dégagé, à partir de longs travaux ayant donné lieu à deux réunions plénières les 12 février 2008 et 5 février 2009 les critères applicables à ce motif : les interceptions de sécurité sollicitées sous le motif « sauvegarde des éléments essentiels du potentiel scientifique et économique de la France » doivent d'une part répondre à une menace (infraction issue du dispositif 411-1 à 411-11 du Code pénal) vérifiable traduisant une intention de nuire aux intérêts d'une entreprise[1] française, d'autre part, la personne dont il est demandé d'intercepter les communications doit être clairement impliquée dans cette menace. L'activité de l'entreprise menacée doit enfin être liée à la défense de notre indépendance nationale[2] au sens de l'article 5 de la Constitution de la Ve République ou à la Sécurité nationale.

Il convient par ailleurs de constater que les pouvoirs publics proposent une approche normative des intérêts économiques et scientifiques constituant une forme de « noyau dur » à protéger prioritairement ainsi que du concept d'intelligence économique, le Décret 2009-1122 du 17 septembre relatif au Délégué interministériel à l'intelligence économique en constituant la dernière illustration.

---

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.
2) 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.

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

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[1] 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 les dernières décisions du Conseil de l'Union européenne en la matière (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. Celui-ci traitait des infractions « commises en bande organisée ». La loi du 9 mars 2004 cependant a cependant 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 1er 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 no 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. Ici encore, la Jurisprudence de la Commission représente une synthèse des dispositifs pénaux qui sont venus constituer le droit positif applicable à cette matière :
– notion de bande organisée au sens de l'article 132-71 du Code pénal ;
– notion d'association de malfaiteurs au sens de l'article 450-1 du Code pénal ;
– notion de « criminalité organisée » au sens de la loi du 9 mars 2004 précitée.

Troisième partie

ÉTUDES ET DOCUMENTS

Chapitre I

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 1er de la loi nº 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 nº 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

	Autorité	Motif	Durée	Renouvellement
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 *NB* : 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 Ier de la loi de 1991.

Loi nº 91-646 du 10 juillet 1991 consolidée

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

Les interceptions ordonnées en matière criminelle et correctionnelle

Code de procédure pénale
Livre Ier : De l'exercice de l'action publique et de l'instruction
Titre III : Des juridictions d'instruction
Chapitre Ier : Du juge d'instruction : juridiction d'instruction du premier degré
Section III : Des transports, des perquisitions, des saisies et des interceptions de correspondances émises par la voie des télécommunications
Sous-section II : Des interceptions de correspondances émises par la voie des télécommunications

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

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

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

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

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

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

Les enregistrements sont placés sous scellés fermés. »

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

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

• Loi nº 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 nº 95-125 du 8 février 1995)* – « Aucune interception ne peut avoir lieu sur la ligne d'un député ou d'un sénateur sans que le président de l'assemblée à laquelle il appartient en soit informé par le juge d'instruction.

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

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

Les interceptions ordonnées pour recherche d'une personne en fuite

Code de procédure pénale
Livre Ier : De l'exercice de l'action publique et de l'instruction
Titre II : Des enquêtes de contrôle d'identité
Chapitre Ier : Des crimes et des délits flagrants

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

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

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

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

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

Code de procédure pénale (loi n° 2002-1138 du 9 septembre 2002, article 66)
Livre I^er^ : De l'exercice de l'action publique et de l'instruction
Titre III : Des juridictions d'instruction
Chapitre I^er^ : 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^er^ du titre III du livre I^er^. 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 no 2007-297 du 5 mars 2007 – article 72 *JORF* 7 mars 2007

« Aux fins de prévenir les évasions et d'assurer la sécurité et le bon ordre des établissements pénitentiaires ou des établissements de santé habilités à recevoir des détenus, les communications téléphoniques 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 nº 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 nº 91-646 du 10 juillet 1991 consolidée) :
DES INTERCEPTIONS DE SÉCURITÉ

Article 3 – « Peuvent être autorisées, à titre exceptionnel, dans les conditions prévues par l'article 4, les interceptions de correspondances 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 nº 2006-64 du 23 janvier 2006* – « L'autorisation est accordée par décision écrite et motivée du Premier ministre ou de l'une des deux personnes spécialement déléguées par lui. Elle est donnée sur proposition écrite et motivée du ministre de la Défense, du ministre de l'Intérieur ou du ministre chargé des Douanes, ou de l'une des deux personnes que chacun d'eux aura spécialement déléguée.

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

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

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

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

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

Cette transcription est effectuée par les personnels habilités. »

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

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

Il est dressé procès-verbal de cette opération. »

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

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

Article 11-1 – *(introduit par l'article 31 de la loi 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 utile. »

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

Textes réglementaires récents visant la loi du 10 juillet 1991

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

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

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

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

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

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

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

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

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

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

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

Article 4 – « La décision mentionnée au premier alinéa de l'article 1er :
a) indique la qualité des agents habilités à demander au fournisseur de prestations de cryptologie la mise en œuvre ou la remise des conventions, ainsi que les modalités selon lesquelles les données à déchiffrer lui sont, le cas échéant, transmises ;
b) fixe le délai dans lequel les opérations doivent être réalisées, les modalités selon lesquelles, dès leur achèvement, le fournisseur remet aux agents visés au a) du présent article les résultats obtenus ainsi que les pièces qui lui ont été éventuellement transmises ;
c) prévoit, dès qu'il apparaît que les opérations sont techniquement impossibles, que le fournisseur remet aux agents visés au a) les pièces qui lui ont été éventuellement transmises. »

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

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

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

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

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

Loi nº 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers

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 nº 2005-532 DC du 19 janvier 2006] les actes de terrorisme, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions peuvent exiger des opérateurs et personnes mentionnés au I de l'article L. 34-1 la communication des données conservées et traitées par ces derniers en application dudit article.

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

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

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

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

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

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

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

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

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

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

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

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

– 4. Il est inséré, dans la même loi, un titre IV ainsi rédigé :

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

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

Cet article appelle les commentaires suivants :

– Sur la « personnalité qualifiée » :

Les demandes relatives à ces données sont soumises à l'appréciation d'une personnalité qualifiée désignée par la Commission pour une durée de trois ans renouvelable, à partir d'une liste de trois noms proposée par le ministre de l'Intérieur. La même procédure est prévue pour la désignation des adjoints de cette personnalité. En application de l'article sus-exposé et du décret 2006-1651 du 22 décembre 2006, la Commission a désigné le 5 novembre 2009 Monsieur Jean ESPITALIER en remplacement de 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 nº 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 nº 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 (3e rapport 1994, p. 19 ; 7e rapport 1998, p. 23 ; 8e rapport 1999, p. 14).

– Sur le contrôle des demandes :

Le texte définitivement adopté stipule que par parallélisme avec les procédures de demandes d'interceptions, les demandes soumises à la Commission seront enregistrées, accompagnées de leur motivation et

communiquées à la Commission. Le décret du 22 décembre 2006 précise que celle-ci peut à tout moment avoir accès aux données enregistrées et demander des éclaircissements sur la motivation des demandes.

Loi n° 2008-1245 du 1er 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.

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 Directeur général de l'Agence nationale de sécurité des systèmes d'information, pièce de la procédure d'autorisation est décrite par ce dispositif (article R. 226-2 du Code pénal).

• **Le décret 2009-619 du 6 juin 2009** relatif à certaines Commissions administratives à caractère consultatif relevant du Premier ministre.

• **Le décret 2009-834 du 7 juillet 2009** portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information » : ce texte confie la Présidence de la Commission dite « R226 » au Directeur général de l'Agence nationale de la sécurité, lui-même rattaché au Secrétariat général de la défense et de la sécurité nationale.

article 4 : L'agence nationale de la sécurité des systèmes d'information se prononce sur la sécurité des dispositifs et des services, offerts par les prestataires, nécessaires à la protection des systèmes d'information.

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

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

• **Le décret 2009-1657 du 24 décembre 2009** relatif au conseil de défense et de sécurité nationale et au secrétariat général de la défense et de la sécurité nationale

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

• **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 œuvrant de manière spécifique le régime relatif au « registre » prévu par l'article R. 226-10 du Code pénal

(registre retraçant la gestion des matériels soumis à autorisation). Cet arrêté a emporté l'abrogation de l'arrêté du 15 janvier 1998 qui constituait jusqu'alors le siège de cette matière ;
– l'instruction du 5 septembre 2006, véritable documentation pédagogique à l'attention des « usagers » de la réglementation relative au matériel. Elle constitue un guide pratique efficace offrant une présentation claire des modalités procédurales d'examen des demandes, ainsi que des règles de compétence de la Commission consultative dite « R. 226 ».

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 SGDN dispose que « Le secrétaire général de la défense nationale instruit les demandes d'autorisation présentées en application de l'article 226-3 du Code pénal. Il préside la Commission chargée d'émettre un avis sur ces demandes d'autorisation ».

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

La présente instruction a pour but de préciser les modalités des procédures d'examen des demandes, la compétence de la Commission consultative chargée de soumettre un avis au Premier ministre ainsi que

le rôle des différents services chargés de fournir des avis techniques et de moralité.

Article 1er
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.[1]

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.

---

1) NB : cette présidence a été confiée au directeur de l'Agence nationale de la sécurité des systèmes d'information à la faveur des décrets du 7 juillet et 24 décembre 2009 précités.

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

Chapitre II

Actualité législative et réglementaire

Décret n° 2009-619 du 6 juin 2009 relatif à certaines commissions administratives à caractère consultatif relevant du Premier ministre

NOR : PRMX0912765D

Le Premier ministre,

Vu la Constitution, notamment son article 37 ;

Vu le décret n° 2006-672 du 8 juin 2006 modifié relatif à la création, à la composition et au fonctionnement de commissions administratives à caractère consultatif ;

Vu le décret n° 2009-613 du 4 juin 2009 modifiant le décret n° 2006-672 du 8 juin 2006 relatif à la création, à la composition et au fonctionnement de commissions administratives à caractère consultatif, notamment son article 4,

Décrète :

Article 1er – Les dispositions réglementaires instituant les commissions administratives à caractère consultatif dont la liste est annexée au présent décret sont prorogées pour une durée de cinq ans.

Article 2 – Le présent décret sera publié au *Journal officiel de la République française*.

ANNEXE

Nom de la commission	Texte institutif
Commission pour l'indemnisation des victimes de spoliations intervenues du fait des législations antisémites en vigueur pendant l'Occupation.	Décret n° 99-778 du 10 septembre 1999 instituant une commission pour l'indemnisation des victimes de spoliations intervenues du fait des législations antisémites en vigueur pendant l'Occupation.
Commission supérieure de codification	Décret n° 89-647 du 12 septembre 1989 relatif à la composition et au fonctionnement de la Commission supérieure de codification.
Conseil national de la vie associative.	Décret n° 2003-1100 du 20 novembre 2003 relatif au Conseil national de la vie associative.
Conseil du développement de la vie associative.	Décret n° 2004-657 du 2 juillet 2004 instituant un conseil du développement de la vie associative.
Commission nationale d'agrément et Commission nationale d'habilitation pour dispenser la formation aux brevets d'aptitude aux fonctions d'animateur et de directeur de centres de vacances et de loisirs.	Décret n° 2002-570 du 22 avril 2002 relatif au Conseil national de l'éducation populaire et de la jeunesse.
Commission chargée de donner un avis sur certaines opérations relatives aux matériels aéronautiques et aux matériels d'armement complexes.	Décret n° 64-1123 du 12 novembre 1964 fixant les conditions d'application de l'article 5 de la loi de finances rectificative pour 1963, modifié par le décret n° 70-388 du 27 avril 1970.
Commission consultative chargée d'émettre un avis sur les matériels susceptibles de porter atteinte à l'intimité de la vie privée et au secret des correspondances.	Article R. 226-2 du code pénal.

Fait à Paris, le 6 juin 2009

François FILLON

Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information »

NOR : PRMD0914748D

Version consolidée au 5 février 2010

Le Premier ministre,

Vu le code de la défense, notamment ses articles R. 1332-2, R. 2311-1 et suivants, D. * 1132-10 et D. 2321-7 ;

Vu le code des postes et des communications électroniques, notamment son article L. 32-1 ;

Vu l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, notamment ses articles 9 et 10 ;

Vu le décret n° 87-389 du 15 juin 1987 modifié relatif à l'organisation des services d'administration centrale ;

Vu le décret n° 92-604 du 1er juillet 1992 modifié portant charte de la déconcentration ;

Vu le décret n° 97-464 du 9 mai 1997 modifié relatif à la création et à l'organisation des services à compétence nationale ;

Vu le décret n° 2001-272 du 30 mars 2001 modifié pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique ;

Vu le décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information ;

Vu le décret n° 2006-672 du 8 juin 2006 modifié relatif à la création, à la composition et au fonctionnement de commissions administratives à caractère consultatif ;

Vu le décret n° 2007-663 du 2 mai 2007 pris pour l'application des articles 30, 31 et 36 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie ;

Vu l'avis du comité technique paritaire spécial du secrétariat général de la défense nationale du 26 mai 2009 ;

Vu l'avis du comité technique paritaire des services du Premier ministre du 25 juin 2009,

Décrète :

Article 1er

Il est créé un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ». Ce service est rattaché au secrétaire général de la défense et de la sécurité nationale.

Article 2

L'Agence nationale de la sécurité des systèmes d'information assiste le secrétaire général de la défense et de la sécurité nationale dans l'exercice de ses attributions dans le domaine de la sécurité des systèmes d'information, notamment celles prévues par le 7° de l'article R. * 1132-3 du code de la défense.

Article 3

L'Agence nationale de la sécurité des systèmes d'information est l'autorité nationale en matière de sécurité des systèmes d'information.

À ce titre :
– elle conçoit, fait réaliser et met en œuvre les moyens interministériels sécurisés de communications électroniques nécessaires au Président de la République et au Gouvernement ;
– elle anime et coordonne les travaux interministériels en matière de sécurité des systèmes d'information ;
– elle élabore les mesures de protection des systèmes d'information proposées au Premier ministre. Elle veille à l'application des mesures adoptées ;
– elle mène des inspections des systèmes d'information des services de l'État ;
– elle met en œuvre un système de détection des évènements susceptibles d'affecter la sécurité des systèmes d'information de l'État et coordonne la réaction à ces évènements. Elle recueille les informations techniques relatives aux incidents affectant les systèmes d'information de l'État ;
– elle délivre des agréments aux dispositifs et aux mécanismes de sécurité destinés à protéger, dans les systèmes d'information, les informations couvertes par le secret de la défense nationale ;
– elle participe aux négociations internationales et assure la liaison avec ses homologues étrangers ;
– elle assure la formation des personnels qualifiés dans le domaine de la sécurité des systèmes d'information.

Article 4

L'Agence nationale de la sécurité des systèmes d'information se prononce sur la sécurité des dispositifs et des services, offerts par les prestataires, nécessaires à la protection des systèmes d'information.

L'agence est en particulier chargée, par délégation du Premier ministre :
– de la qualification des produits de sécurité et de prestataires de services de confiance ainsi que de l'habilitation des organismes prévue par le décret n° 2010-112 du 2 février 2010 ;
– de la certification de sécurité des dispositifs de création et de vérification de signature électronique prévue par le décret du 30 mars 2001 susvisé ;
– de l'agrément des centres d'évaluation et de la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information prévus par le décret du 18 avril 2002 susvisé ;
– de la délivrance des autorisations et de la gestion des déclarations relatives aux moyens et aux prestations de cryptologie prévues par le décret du 2 mai 2007 susvisé.

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

Article 5

L'Agence nationale de la sécurité des systèmes d'information apporte son concours aux services de l'État en matière de sécurité des systèmes d'information.

Elle apporte son soutien :
– au ministre chargé des communications électroniques dans le domaine de l'intégrité et de la sécurité des réseaux de communications électroniques ouverts au public ;
– aux ministres coordonnateurs des secteurs d'activité d'importance vitale pour la protection de la sécurité des systèmes d'information des installations d'importance vitale.

Article 6

L'Agence nationale de la sécurité des systèmes d'information favorise la prise en compte de la sécurité dans le développement des technologies de l'information et de la communication.

Elle participe à l'orientation de la recherche, des études et du développement des dispositifs et des technologies de la sécurité des systèmes d'information.

Elle contribue à la promotion des technologies et des savoir-faire nationaux en matière de sécurité des systèmes d'information.

Article 7

Il est institué auprès du secrétaire général de la défense et de la sécurité nationale un comité stratégique de la sécurité des systèmes d'information. Ce comité propose les orientations stratégiques en matière de sécurité des systèmes d'information et en suit la mise en œuvre.

Outre le secrétaire général de la défense et de la sécurité nationale qui en assure la présidence, le comité comprend :
– le chef d'état-major des armées ;
– le secrétaire général du ministère de l'intérieur, de l'outre-mer et des collectivités territoriales ;
– le secrétaire général du ministère des affaires étrangères et européennes ;
– le délégué général pour l'armement ;
– le directeur général de la sécurité extérieure ;
– le directeur général des systèmes d'information et de communication ;
– le directeur général de la modernisation de l'État ;
– le directeur central du renseignement intérieur ;
– le vice-président du Conseil général de l'industrie, de l'énergie et des technologies ;
– le directeur général de l'Agence nationale de la sécurité des systèmes d'information.

Le secrétaire général de la défense et de la sécurité nationale peut convier des personnalités qualifiées.

L'Agence nationale de la sécurité des systèmes d'information assure le secrétariat du comité.

Article 8

L'Agence nationale de la sécurité des systèmes d'information dispose, sur les crédits gérés par le secrétariat général de la défense et de la sécurité nationale, des moyens nécessaires à l'accomplissement de ses missions.

Article 9

Dans toutes les dispositions à caractère réglementaire, la référence à la direction centrale de la sécurité des systèmes d'information est remplacée par la référence à l'Agence nationale de la sécurité des systèmes d'information.

Article 10

Le décret nº 2001-693 du 31 juillet 2001 créant au secrétariat général de la défense nationale une direction centrale de la sécurité des systèmes d'information et l'article D. 1132-9 du code de la défense sont abrogés.

Article 11

Le ministre du budget, des comptes publics, 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*.

Fait Paris, le 7 juillet 2009.
François Fillon
Par le Premier ministre :
Le ministre du budget, des comptes publics,
de la fonction publique
et de la réforme de l'État,
Éric Woerth

Décret n° 2009-1657 du 24 décembre 2009 relatif au conseil de défense et de sécurité nationale et au secrétariat général de la défense et de la sécurité nationale

NOR : PRMX0928467D

Le Président de la République,

Sur le rapport du Premier ministre,

Vu la Constitution, notamment ses articles 15, 20 et 21 ;

Vu le code de la défense ;

Vu le code pénal ;

Vu la loi nº 2007-1443 du 9 octobre 2007 portant création d'une délégation parlementaire au renseignement ;

Vu le décret nº 2009-752 du 23 juin 2009 relatif à l'Institut des hautes études de défense nationale ;

Vu le décret nº 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information » ;

Vu le décret nº 2009-1122 du 17 septembre 2009 relatif au délégué interministériel à l'intelligence économique ;

Vu le décret nº 2009-1321 du 28 octobre 2009 relatif à l'Institut national des hautes études de la sécurité et de la justice ;

Vu l'avis du comité technique paritaire ministériel des services du Premier ministre en date du 26 novembre 2009 ;

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

Le conseil des ministres entendu,

Décrète :

Article 1er

La section unique du chapitre II du titre II du livre Ier de la partie 1 de la partie réglementaire du code de la défense est remplacée par les dispositions suivantes :

« Section unique

« Conseil de défense et de sécurité nationale

« Sous-section 1

« Dispositions générales

« Art. R. * 1122-1.-Le conseil de défense et de sécurité nationale définit les orientations en matière de programmation militaire, de dissuasion, de conduite des opérations extérieures, de planification des réponses aux crises majeures, de renseignement, de sécurité économique et énergétique, de programmation de sécurité intérieure concourant à la sécurité nationale et de lutte contre le terrorisme. Il en fixe les priorités.

« Art. R. * 1122-2.-Dans sa formation plénière, le conseil de défense et de sécurité nationale comprend, outre le Président de la République, qui le préside :

« 1° Le Premier ministre ;

« 2° Le ministre de la Défense ;

« 3° Le ministre de l'Intérieur ;

« 4° Le ministre chargé de l'économie ;

« 5° Le ministre chargé du budget ;

« 6° Le ministre des affaires étrangères,

et, s'il y a lieu, sur convocation du président, d'autres ministres pour les questions relevant de leur responsabilité.

« Art. R. * 1122-3.-Le conseil de défense et de sécurité nationale peut être réuni en conseil restreint, dans une composition fixée par son président en fonction des points figurant à son ordre du jour. Il peut également être réuni en formation spécialisée.

« Art. R. * 1122-4.-Le président du conseil de défense et de sécurité nationale peut, en outre, convoquer pour être entendue par le conseil, en formations plénière, spécialisées ou restreintes, toute personnalité en raison de sa compétence.

« Art. R. * 1122-5.-Le secrétariat du conseil de défense et de sécurité nationale, dans ses formations plénières, spécialisées et restreintes, est assuré par le secrétaire général de la défense et de la sécurité nationale.

« Sous-section 2

« Conseil national du renseignement

« Art. R. * 1122-6.-Le conseil national du renseignement constitue une formation spécialisée du conseil de défense et de sécurité nationale.

« Le conseil national du renseignement définit les orientations stratégiques et les priorités en matière de renseignement. Il établit la planification des moyens humains et techniques des services spécialisés de renseignement.

« Art. R. * 1122-7.-Siègent au conseil national du renseignement, sous la présidence du Président de la République, le Premier ministre,

les ministres et les directeurs des services spécialisés de renseignement dont la présence est requise par l'ordre du jour ainsi que le coordonnateur national du renseignement.

« Art. R. * 1122-8.-Nommé par décret en conseil des ministres, le coordonnateur national du renseignement conseille le Président de la République dans le domaine du renseignement.

« Avec le concours du secrétaire général de la défense et de la sécurité nationale, le coordonnateur national du renseignement rapporte devant le conseil national du renseignement dont il prépare les réunions et il veille à la mise en œuvre des décisions prises par le conseil.

« Il coordonne l'action et s'assure de la bonne coopération des services spécialisés constituant la communauté française du renseignement.

« Il transmet les instructions du Président de la République aux responsables de ces services, qui, lui communiquent les renseignements devant être portés à la connaissance du Président de la République et du Premier ministre, et lui rendent compte de leur activité.

« Le coordonnateur national du renseignement peut être entendu par la délégation parlementaire au renseignement.

« Sous-section 3

« Conseil des armements nucléaires

« Art. R. * 1122-9.-Le conseil des armements nucléaires constitue une formation spécialisée du conseil de défense et de sécurité nationale.

« Le conseil des armements nucléaires définit les orientations stratégiques et s'assure de l'avancement des programmes en matière de dissuasion nucléaire.

« Art. R. * 1122-10.-Siègent au conseil des armements nucléaires, sous la présidence du Président de la République, le Premier ministre, le ministre de la défense, le chef d'état-major des armées, le délégué général pour l'armement et le directeur des applications militaires du commissariat à l'énergie atomique. »

Article 2

La section I du chapitre II du titre III du livre Ier de la partie 1 de la partie réglementaire du code de la défense est remplacée par les dispositions suivantes :

« Section 1

« Secrétariat général de la défense et de la sécurité nationale

« Art. R. * 1132-1.-Le secrétariat général de la défense et de la sécurité nationale constitue un service du Premier ministre.

« Art. R. * 1132-2.-Le secrétaire général de la défense et de la sécurité nationale assure le secrétariat du conseil de défense et de sécurité nationale. Conformément aux directives du Président de la République et du Premier ministre, il conduit, en liaison avec les départements ministériels concernés, les travaux préparatoires aux réunions. Il prépare les relevés de décisions, notifie les décisions prises et en suit l'exécution.

« Art. R. * 1132-3.-Le secrétaire général de la défense et de la sécurité nationale assiste le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. À ce titre :

« 1° Il anime et coordonne les travaux interministériels relatifs à la politique de défense et de sécurité nationale et aux politiques publiques qui y concourent ;

« 2° En liaison avec les départements ministériels concernés, il suit l'évolution des crises et des conflits internationaux pouvant affecter les intérêts de la France en matière de défense et de sécurité nationale et étudie les dispositions susceptibles d'être prises. Il est associé à la préparation et au déroulement des négociations ou des réunions internationales ayant des implications sur la défense et la sécurité nationale et est tenu informé de leurs résultats ;

« 3° Il propose, diffuse et fait appliquer et contrôler les mesures nécessaires à la protection du secret de la défense nationale. Il prépare la réglementation interministérielle en matière de défense et de sécurité nationale, en assure la diffusion et en suit l'application ;

« 4° En appui du coordonnateur national du renseignement, il concourt à l'adaptation du cadre juridique dans lequel s'inscrit l'action des services de renseignement et à la planification de leurs moyens et assure l'organisation des groupes interministériels d'analyse et de synthèse en matière de renseignement ;

« 5° Il élabore la planification interministérielle de défense et de sécurité nationale, veille à son application et conduit des exercices interministériels la mettant en œuvre. Il coordonne la préparation et la mise en œuvre des mesures de défense et de sécurité nationale incombant aux divers départements ministériels et s'assure de la coordination des moyens civils et militaires prévus en cas de crise majeure ;

« 6° Il s'assure que le Président de la République et le Gouvernement disposent des moyens de commandement et de communications électroniques nécessaires en matière de défense et de sécurité nationale et en fait assurer le fonctionnement ;

« 7° Il propose au Premier ministre et met en œuvre la politique du Gouvernement en matière de sécurité des systèmes d'information. Il dispose à cette fin du service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information" ;

« 8° Il veille à la cohérence des actions entreprises en matière de politique de recherche scientifique et de projets technologiques intéressant la défense et la sécurité nationale et contribue à la protection des intérêts nationaux stratégiques dans ce domaine.

« Art. D. 1132-4.-Par délégation du Premier ministre, le secrétaire général de la défense et de la sécurité nationale préside les instances interministérielles chargées d'étudier, avant décision gouvernementale, les questions relatives aux exportations d'armement, de matériels et de technologies de caractère stratégique. Il en assure le secrétariat. Il suit la mise en œuvre des procédures interministérielles destinées au contrôle de cessions de matières, de matériels et de technologies de caractère sensible.

« Art. D. 1132-5.-Le secrétaire général de la défense et de la sécurité nationale peut signer, au nom du Premier ministre et par délégation, l'ensemble des actes, à l'exception des décrets, relatifs aux affaires mentionnées à la présente section.

« Art. D. 1132-6.-Par délégation du Premier ministre, le secrétaire général de la défense et de la sécurité nationale assure la tutelle de l'Institut des hautes études de défense nationale et de l'Institut national des hautes études de la sécurité et de la justice. »

Article 3

Les personnels civils et militaires, titulaires et non titulaires, nommés et affectés avant la publication du présent décret au secrétariat général de la défense nationale, sont réputés avoir été, dans les mêmes conditions statutaires, nommés et affectés au secrétariat général de la défense et de la sécurité nationale. Ils conservent l'ancienneté acquise dans leur précédente situation.

Article 4

I. – La partie réglementaire du code de la défense est ainsi modifiée :

1° La sous-section 1, intitulée « Comité d'action scientifique de la défense », de la section 3 du chapitre II du titre III du livre Ier de la partie 1 est supprimée et les articles D. 1132-34 à D. 1132-38 sont abrogés ;

2° La sous-section 2, intitulée « Comité interministériel du renseignement », de la section 3 du chapitre II du titre III du livre Ier de la partie 1 est supprimée et les articles D. * 1132-39 à D. * 1132-42 sont abrogés ;

3° La sous-section 3, intitulée « Commission interministérielle de coordination des instances de contrôle des transferts intéressant la défense et la sécurité, » de la section 3 du chapitre II du titre III du livre Ier de la partie 1 est supprimée et les articles D. 1132-43 à D. 1132-47 sont abrogés ;

4° La sous-section 7, intitulée « Commission interministérielle pour la sécurité des systèmes d'information », de la section 3 du chapitre II du titre III du livre Ier de la partie 1 ainsi que la section unique, intitulée « Commission interministérielle pour la sécurité des systèmes d'information », du chapitre Ier du titre II du livre III de la partie 2 sont supprimées et les articles D. 1132-55 et D. 2321-1 à D. 2321-7 sont abrogés ;

5° La sous-section 1, intitulée « Commission de défense nationale des carburants », de la section 2 du chapitre VI du titre III du livre III de la partie 1 est supprimée et les articles D. 1336-43 à D. 1336-46 sont abrogés ;

6° Aux 1° des articles R. 1631-3, R. 1641-2, R. 1651-3, R. 1661-3 et R. 1671-3, les références : « R. 1132-1 à R. 1132-3, » sont supprimées ;

7° Aux 1° des articles D. * 1631-5, D. * 1641-4, D. * 1651-5, D. * 1661-5 et D. * 1671-5, les références : « D. * 1132-10 » et « D. * 1132-55 » sont supprimées ;

8° Les 1° des articles D. 1631-6, D. 1641-5, D. 1651-6, D. 1661-6 et D. 1671-6 sont remplacés par les dispositions suivantes :

« 1° Au livre Ier, les dispositions des articles D. 1132-53, D. 1132-54, D. 1142-30 à D. 1142-34, D. 1143-9 à D. 1143-13 ; »

9° Aux 2° des articles D. 1631-6, D. 1641-5, D. 1651-6, D. 1661-6 et D. 1671-6, les références : « D. 1336-43 à D. 1336-46, » sont supprimées ;

10° Aux 2° des articles D. 2441-3, D. 2451-3, D. 2461-4 et D. 2471-5, les références : « D. 2321-1 à D. 2321-7 » sont supprimées.

II. – Le décret no 2002-890 du 15 mai 2002 relatif au conseil de sécurité intérieure est abrogé.

Article 5

I. – À l'article 2 du décret du 7 juillet 2009 susvisé, la référence : « l'article D. * 1132-10 » est remplacée par la référence : « le 7° de l'article R. * 1132-3 ».

II. – Dans les articles R. 226-2, R. 226-4 et R. 226-8 du code pénal, les mots : « secrétaire général de la défense nationale » sont remplacés par les mots : « directeur général de l'Agence nationale de la sécurité des systèmes d'information » et dans l'article 226-2 du même code, les mots : « le secrétariat général de la défense nationale » sont remplacés par les mots : « l'Agence nationale de la sécurité des systèmes d'information ».

III. – Dans toutes les dispositions à caractère réglementaire, sous réserve des dispositions du II du présent article, les références au conseil de défense, au secrétariat général de la défense nationale et au secrétaire général de la défense nationale sont remplacées respectivement par les références au conseil de défense et de sécurité nationale, au secrétariat général de la défense et de la sécurité nationale et au secrétaire général de la défense et de la sécurité nationale.

Article 6

Les dispositions des articles D. 1132-4 à D. 1132-6 de la section 1 du chapitre II du titre III du livre Ier de la partie 1 de la partie réglementaire du code de la défense mentionnées à l'article 3 du présent décret peuvent être modifiées par décret.

Article 7

Les dispositions du présent décret entrent en vigueur le 13 janvier 2010.

Article 8

Le Premier ministre, le ministre des affaires étrangères et européennes, la ministre de l'économie, de l'industrie et de l'emploi, le ministre de l'intérieur, de l'outre-mer et des collectivités territoriales, le ministre du budget, des comptes publics, de la fonction publique et de la réforme de l'État et le ministre de la défense sont responsables, chacun en ce qui le concerne, de l'application du présent décret, qui sera publié au *Journal officiel de la République française.*

Fait à Paris,
le 24 décembre 2009.

Chapitre III

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).

Chapitre IV

Questions parlementaires Éléments de jurisprudence

Questions parlementaires

Droits de l'homme et libertés publiques (écoutes téléphoniques – coût – statistiques)

52035. – 16 juin 2009. – M. Jean-Jacques URVOAS attire l'attention de Mme la garde des Sceaux, Ministre de la Justice, sur le coût des écoutes de téléphones portables par la suite à l'ouverture d'une commission rogatoire. Selon des informations diffusées par la presse, chacune de ces écoutes serait en effet facturée 700 euros mensuellement par les opérateurs. D'autre part, les lignes dérivées vers les centraux d'écoute des services de police judiciaire seraient traitées par l'entremise d'un matériel lui-même loué à l'année à des sociétés privées. Il l'interroge dès lors sur le coût global de ces différents dispositifs pour l'État.

Réponse. – La question de la réduction des frais de justice en matière de réquisitions aux opérateurs de communications électroniques, y compris les coûts des interceptions judiciaires de communications électroniques autorisées par les magistrats, constitue une priorité d'action du ministère de la justice et des libertés. Le coût unitaire d'une interception des communications de téléphonie mobile s'établit aujourd'hui à 88 euros hors taxe, quelle que soit la durée de l'interception pour le coût lié à la mise en place de l'interception par l'opérateur de communications électroniques, d'une part, et de 10,85 à 17 euros hors taxe par jour pour le coût lié à la location de la centrale d'écoutes, d'autre part. Afin d'adapter les moyens d'interception aux évolutions des usages et des technologies en matière de communications électroniques ainsi que de diminuer significativement le montant des frais de justice, les

services de la chancellerie conduisent actuellement le projet de création d'une plate-forme nationale des interceptions judiciaires. Parallèlement, des travaux interministériels sont en cours pour instaurer une tarification des prestations appliquées au domaine de l'Internet.

Système pénitentiaire
(établissements – sécurité – téléphonie – accès – détenus)

52598. – 16 juin 2009. – M. François-Michel GONNOT interroge Mme la garde des Sceaux, Ministre de la Justice, sur les circonstances dans lesquelles un terroriste, emprisonné à la centrale de Poissy, a pu téléphoner en direct, depuis sa prison, au candidat D. qui tenait un meeting pendant la campagne des élections européennes. Il aimerait savoir dans quelles conditions exactement ce détenu peut téléphoner, et à quelles personnes, et comment l'administration a-t-elle pu laisser un tel prisonnier appeler ce jour-là, sans contrôle. Il exige que les conclusions de l'enquête qui a été demandée soient rendues publiques et demande les mesures que le Gouvernement compte prendre pour que de telles fautes ne se reproduisent plus.

Réponse. – L'accès à la téléphonie est un droit de la personne détenue condamnée consacré par la règle pénitentiaire européenne (RPE) 24.1 relative aux contacts avec le monde extérieur et par l'article 727-1 du code de procédure pénale. Dans le cadre de la mise en œuvre des RPE, la direction de l'administration pénitentiaire a décidé de permettre cet accès non seulement en établissements pour peine (maisons centrales et centres de détention), mais également en maison d'arrêt. Ainsi, l'ensemble des maisons d'arrêt est progressivement équipé de points phone localisés en coursive ou en cours de promenade, à l'instar des établissements pour peine. Le règlement intérieur fixe la fréquence et la durée des communications. Si des cabines téléphoniques sont installées, le détenu doit demander l'attribution d'un code d'accès personnalisé. Le personnel peut écouter la conversation d'un détenu ou même l'enregistrer, sauf s'il s'agit d'une conversation avec l'avocat dudit détenu. La conversation peut être interrompue si elle présente un risque d'atteinte à la sécurité de l'établissement ou aux personnes détenues. La communication téléphonique, au cours de laquelle un détenu condamné pour des faits de terrorisme a pu s'entretenir pendant plusieurs minutes avec les participants d'une réunion publique inscrite dans le contexte d'un scrutin européen, n'a pas été interrompue, en raison d'une surveillance discontinue de l'écoute. À cette première cause s'ajoute le système d'appel en vigueur qui offrait une relative latitude d'appels aux détenus en leur permettant de joindre une très grande variété d'interlocuteurs, à la seule condition que les numéros de ceux-ci n'aient pas été préalablement identifiés comme étant inscrits sur la liste noire correspondant à des numéros interdits. À la suite de cet incident, plusieurs mesures ont immédiatement été prises au plan local permettant de réguler cette situation. Le directeur de la maison centrale de Poissy a ainsi rappelé aux agents en charge des écoutes téléphoniques, d'une part, que le suivi des appels émis par

une personne détenue signalée était prioritaire. D'autre part, l'obligation de couper immédiatement la communication s'il existe des éléments de nature à être divulgués dans les médias a été réaffirmée. Par ailleurs, il a été procédé à l'inscription sur la liste noire des numéros incriminés lors de l'incident signalé. La circulaire du 13 juillet 2009 concernant l'usage du téléphone par les personnes détenues condamnées pose désormais le principe de la liste nominative dans tous les établissements pénitentiaires : la personne détenue ne peut appeler que des numéros autorisés préalablement par le chef d'établissement, sur justificatifs à chaque correspondant. Le dispositif dit « de liste nominative » sera effectif dans tous les établissements pénitentiaires au cours des prochaines semaines.

Système pénitentiaire
(détenus – téléphonie – accès)

63463. 10 novembre 2009. – Mme Marietta Karamanli attire l'attention de Mme la Ministre d'État, garde des Sceaux, ministre de la Justice et des Libertés, sur la situation des détenus au regard de l'utilisation du téléphone. L'article 39 de la loi pénitentiaire tel qu'adopté par le Parlement prévoit que les personnes détenues ont le droit de téléphoner aux membres de leur famille. Elles peuvent être autorisées à téléphoner à d'autres personnes pour préparer leur réinsertion. Dans tous les cas, les prévenus doivent obtenir l'autorisation de l'autorité judiciaire. L'accès au téléphone peut être refusé, suspendu ou retiré, pour des motifs liés au maintien du bon ordre et de la sécurité ou à la prévention des infractions et, en ce qui concerne les prévenus, aux nécessités de l'information. Actuellement, une note de l'administration pénitentiaire fixe à quarante le nombre de personnes pouvant être appelées hors les avocats de la personne détenue. Ce nombre de personnes peut être inférieur au nombre des personnes disposant d'un permis de visite. De plus les tarifs pratiqués paraissent être parfois beaucoup plus élevés qu'à l'extérieur. Si certains établissements permettent aux détenus de recourir à des dispositifs utilisant Internet, ce qui est de nature à diminuer le coût des communications passées, cette facilité suppose que les personnes appelées aient eux-mêmes accès à Internet, ce qui n'est pas toujours le cas. Enfin les détenus d'origine étrangère ou des DOM TOM ne peuvent téléphoner que de jour ici, ce qui veut dire à des tarifs très élevés. D'une part, elle lui demande s'il ne conviendrait pas que le nombre de possibles correspondants téléphoniques des personnes détenues ne soit pas limité a priori sauf exception justifiée par une impossibilité matérielle technique ou par le caractère anormal de la demande de la personne détenue. D'autre part, elle souhaiterait savoir si l'administration pénitentiaire entend prendre des dispositions permettant un accès au téléphone à des tarifs raisonnables et accessibles pour l'ensemble des détenus les autorisant de la sorte à préserver les liens familiaux, amicaux ou sociaux de nature à leur permettre d'assurer leur réinsertion.

Réponse. – L'accès à la téléphonie est un droit de la personne détenue condamnée consacré par la règle pénitentiaire européenne (RPE) 24.1

relative aux contacts avec le monde extérieur et par l'article 727-1 du code de procédure pénale. Dans le cadre de la mise en œuvre des RPE, la direction de l'administration pénitentiaire a décidé de permettre cet accès non seulement en établissements pour peine (maisons centrales et centre de détention), mais également en maisons d'arrêt. Ainsi, l'ensemble des maisons d'arrêt est progressivement équipé de points phone localisés en coursive ou en cours de promenade, à l'instar des établissements pour peine. Le règlement intérieur fixe la fréquence et la durée des communications. Si des cabines téléphoniques sont installées, le détenu doit demander l'attribution d'un code d'accès personnalisé. La règle en vigueur depuis la circulaire du 13 juillet 2009 est celle de l'autorisation individuelle de téléphoner délivrée par le chef d'établissement à hauteur de 20 numéros pour les condamnés en maisons d'arrêt et de 40 numéros pour les condamnés en établissement pour peine. En complément de cette liste individuelle de numéros, chaque chef d'établissement établit, en collaboration avec le service pénitentiaire d'insertion et de probation, une liste de numéros communs que tous les détenus peuvent appeler, tels des correspondants permettant de préparer un aménagement de peine ou la sortie. Par ailleurs, le détenu peut avoir accès, à titre gratuit et en toute confidentialité à Croix rouge écoute détenu (CRED) et à l'Association réflexion action prison et justice (ARAPEJ). Le nombre de correspondants en maisons d'arrêt a été fixé, conformément à la moyenne constatée dans ces établissements et doit permettre aux services concernés de traiter les demandes quotidiennes. Ce même souci d'instruction rapide des demandes explique le dispositif allégé de contrôle des pièces justificatives instauré en maison d'arrêt, sauf pour les profils particuliers. Ce dispositif doit permettre un accès effectif des personnes détenues au téléphone. L'accès au téléphone des condamnés à un tarif raisonnable est une des préoccupations de l'administration pénitentiaire, formalisée par les dispositions contractuelles liant le délégataire. La facturation des communications téléphoniques effectuées par les détenus est alignée sur les tarifs de France Télécom avec une remise de base de 15,73 %. Des remises sont également appliquées selon le volume des unités consommées par l'ensemble des détenus sur un mois. Pour les détenus indigents, une aide financière est accordée dans certains établissements pénitentiaires par la commission d'indigence. De plus, un dispositif sera mis en place à compter du 1er janvier 2010 afin de permettre aux détenus arrivants de téléphoner gratuitement dans les premières heures de leur arrivée à l'établissement. Enfin, pour une parfaite information des détenus, les tarifs des communications doivent être portés à la connaissance des utilisateurs par un affichage clair et précis de chaque poste téléphonique.

Éléments de jurisprudence

Jurisprudence européenne

Procès équitable/égalité des armes

• Refus du tribunal de communiquer à la défense les documents relatifs à une opération de surveillance et d'accepter les dépositions de témoins clés obtenues par la défense : violation.

Mirilachvili – Russie (n° 6293/04)

Arrêt 11.12.2008 [Section I]

En fait : en 2003, le requérant fut reconnu coupable d'avoir organisé l'enlèvement d'un groupe de personnes. Le tribunal s'appuya sur des enregistrements de conversations téléphoniques réalisés par la police dans l'appartement de l'une des victimes. Au nom de la loi sur les activités opérationnelles et d'enquête, le tribunal refusa de communiquer à la défense les pièces touchant à l'autorisation des écoutes. Le tribunal attacha également une grande importance aux témoignages écrits de trois témoins majeurs, lesquels témoignages avaient été obtenus par un enquêteur au stade préliminaire et lus lors du procès. Ces témoins résidaient en Géorgie et le tribunal demanda donc aux autorités géorgiennes d'assurer la comparution de ces témoins à l'audience mais en vain. Deux des témoins ne se présentèrent jamais devant les juridictions russes et le troisième ne comparut qu'au procès en appel. Le requérant n'eut pas non plus la possibilité de questionner ces témoins lors de l'enquête préliminaire. Toutefois, les trois témoins furent interrogés en Géorgie par les avocats de la défense après le début du procès et envoyèrent au tribunal des dépositions écrites dans lesquelles ils revenaient sur leurs premiers aveux. Tous déclarèrent avoir accusé le requérant à tort et avoir fait leurs dépositions antérieures devant le parquet sous la contrainte. La défense demanda au tribunal d'accueillir ces dépositions mais le tribunal s'y opposa au motif que la loi interdisait à la défense d'interroger des témoins déjà entendus par le ministère public et d'une manière non-conforme à la procédure de recueil des preuves « en bonne et due forme » requise par la loi. Pour l'essentiel, la condamnation du requérant fut confirmée en appel.

En droit : refus de divulgation de pièces à la défense : La Cour n'exclut pas la possibilité que les pièces en cause aient pu être utiles à la défense, laquelle aurait donc eu un intérêt légitime à en demander la communication. Elle est toutefois disposée à admettre, au vu du contexte de l'affaire, que les documents réclamés par le requérant pouvaient comporter certaines informations sensibles touchant à la sécurité nationale. Dans ces conditions, le juge national jouit d'une large marge d'appréciation pour se prononcer sur la demande de divulgation présentée par la défense. La question se pose de savoir si la non-divulgation a été contrebalancée par des garanties procédurales adéquates. Les pièces liées à l'autorisation des écoutes téléphoniques ont été examinées par le président de l'audience de manière non contradictoire. Dès lors, le refus de divulguer certaines

informations n'a pas été une décision unilatérale du ministère public mais celle d'un juge. Toutefois, le tribunal n'a pas examiné si les documents auraient pu être d'une aide quelconque pour la défense ou si leur divulgation aurait pu, du moins de manière défendable, léser un intérêt public. Le tribunal a fondé sa décision sur la nature des pièces en cause et non sur une analyse de leur contenu. Au vu de la loi sur les activités opérationnelles et d'enquête qui interdit en termes absolus la divulgation d'informations touchant auxdites activités, le rôle du tribunal lors de l'examen de la demande de divulgation présentée par la défense a été des plus limités. Le processus décisionnel a donc été lourdement vicié. La décision attaquée était vague et ne précisait pas le genre d'informations sensibles que pouvaient contenir les documents relatifs à l'opération de surveillance. Le tribunal a admis l'exclusion pure et simple d'un examen contradictoire de toutes les pièces. Par ailleurs, l'opération de surveillance ne visait pas le requérant ou son coinculpé. Somme toute, la décision de ne pas communiquer les pièces touchant à l'opération de surveillance n'a pas été assortie de garanties procédurales adéquates ni suffisamment fondée.

Recevabilité des dépositions des témoins : La défense a été placée dans une position désavantageuse vis-à-vis de l'accusation : le ministère public a été en mesure d'interroger directement les témoins-clés, ce que n'a pas pu faire la défense. Toutefois l'impossibilité, pour le requérant, d'interroger ces témoins en personne peut s'expliquer par certaines circonstances objectives échappant au contrôle des autorités russes. Il n'en demeure pas moins que ce fait, à lui tout seul, ne suffit pas pour permettre de conclure à l'équité de l'administration et de l'examen des preuves. La défense n'a pas eu l'autorisation de produire de nouvelles dépositions écrites des témoins. Les preuves soumises par la défense étaient pertinentes et importantes. Les trois témoins en cause étaient des témoins à charge essentiels. La défense se promettait de leurs nouvelles dépositions la possibilité non seulement d'obtenir des preuves absolutoires mais aussi de contester les preuves à charge contre le requérant. À l'appui de son refus d'examiner de nouvelles dépositions, le tribunal a invoqué une disposition de loi interne qui ne semble pas poursuivre un quelconque intérêt légitime identifiable. Dans les circonstances particulières de l'espèce où le requérant n'a pas été à même d'interroger plusieurs témoins clés à l'audience ou au moins lors de la phase préliminaire, le refus d'admettre les déclarations obtenues par la défense n'est pas justifiée. La Cour souligne cependant qu'elle n'entend pas, par ce constat, se prononcer sur l'appréciation de ce moyen de preuve, laquelle appréciation est une prérogative des juridictions internes.

Équité globale de la procédure : La défense a été soigneusement désavantagée vis-à-vis de l'accusation s'agissant de l'examen d'une partie très importante du dossier. Au vu du rôle que jouent les apparences en matière de justice pénale, la procédure en cause, prise dans son ensemble, n'a pas satisfait aux exigences d'un « procès équitable ».

Conclusion : violation (unanimité).

Jurisprudence française

– Art. 76-97 CPP – Cour de cassation – CRIM – 13 novembre 2008

Vu le mémoire produit, commun aux demandeurs ;

• Attendu qu'il résulte de l'arrêt attaqué et des pièces de la procédure que, dans l'information suivie contre personne non dénommée des chefs, notamment, de vols, blanchiment et escroquerie en bande organisée, le juge d'instruction a, par ordonnance du 6 avril 2007, autorisé la mise en place d'un dispositif technique de sonorisation et de captation d'images dans l'habitation de Serge L. ; que, par ordonnance du 10 avril 2007, le juge des libertés et de la détention a autorisé les enquêteurs à s'introduire dans ces lieux, en dehors des heures légales, afin d'y placer le dispositif ; que, le 16 avril 2007, le juge d'instruction a donné commission rogatoire au commandant de la section recherche de la gendarmerie de Paris afin de procéder à la mise en place de ce dispositif technique pour une période effective de deux mois ; que des enregistrements ont été effectués entre le 23 avril et le 20 juin 2007 ; que, par une deuxième ordonnance du 5 juillet 2007, le juge d'instruction a autorisé les officiers de police judiciaire à prolonger le dispositif technique ; que, pour l'exécution de cette décision, le magistrat instructeur a délivré le même jour une commission rogatoire fixant à une période affective de deux mois la durée des mesures autorisées ; que, par une troisième ordonnance du 31 août 2007, le juge d'instruction a autorisé la prolongation du dispositif technique pour une nouvelle et ultime durée effective de quatre mois ; qu'une commission rogatoire délivrée le même jour a également fixé à quatre mois la durée du fonctionnement du dispositif ;

• Attendu que Serge L., François D., Yassine F., James T. et Jessica S. ont été mis en examen le 30 novembre 2007 ; qu'ils ont saisi la chambre de l'instruction de requêtes tendant, notamment, à l'annulation de la procédure de sonorisation et de captation d'images au domicile de Serge L. ; que l'arrêt attaqué a dit n'y avoir lieu à annulation d'un acte ou d'une pièce de la procédure ;

En cet état :

Sur le premier moyen de cassation, pris de la violation des articles 706-96, 706-97, 802 du Code de procédure pénale, 8 de la Convention européenne des droits de l'homme, ensemble violation des droits de la défense ; (...)

• Attendu que, pour rejeter les moyens d'annulation proposés par les demandeurs, pris de l'absence, dans les ordonnances du juge d'instruction des 6 avril et 5 juillet 2007 autorisant la sonorisation et la captation d'images au domicile de Serge L., de toute mention relative à la durée de ces mesures, l'arrêt énonce que les commissions rogatoires des 16 avril et 5 juillet 2007 ont fixé la durée de leur exécution à deux mois ; que les juges retiennent que l'ordonnance d'autorisation constitue, avec

la commission rogatoire délivrée pour son exécution, la décision prévue par l'article 706-97 du Code de procédure pénale ;

• Attendu qu'en cet état, la chambre de l'instruction a justifié sa décision ;

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

Mais, sur le deuxième moyen de cassation, pris de la violation des articles 706-96, 706-97, 706-101, 802 du Code de procédure pénale, 8 de la Convention européenne des droits de l'homme, ensemble violation des droits de la défense ;

« en ce que l'arrêt attaqué a refusé de constater la nullité des opérations de sonorisation, de leur retranscription et de toute la procédure subséquente à compter au moins du 6 juin 2007 ainsi que la nullité des ordonnances du 5 juillet et du 31 août 2007 ;

« aux motifs qu'il résulte de l'article 706-97 que la durée mentionnée est celle des mesures ordonnées soit en l'espèce, l'installation d'un dispositif de sonorisation et de captation d'images au domicile de Serge L. ; qu'il s'ensuit, contrairement à ce qui est soutenu par les demandeurs, que la durée desdites mesures s'apprécie à partir de leur mise en place et non à partir de la décision les autorisant ; qu'en toute hypothèse, le juge d'instruction a précisé à la commission rogatoire fixant la durée des mesures qu'il s'agissait « d'une période effective de deux mois » ; que, dès lors, le dispositif ayant été installé le 20 avril 2007, la mesure s'est régulièrement achevée le 20 juin 2007 ; qu'en conséquence, aucune irrégularité initiale tenant au point de départ du calcul de la durée de la sonorisation initiale n'est constatée et les ordonnances de prolongation de la mesure du 5 juillet et du 31 août n'encourent pas la critique de ce chef ;

« alors que l'article 706-96 du Code de procédure pénale exige que les opérations de sonorisation dans un lieu privé et a fortiori dans un domicile privé soient effectuées sous le contrôle et l'autorité du juge d'instruction ; que le point de départ de la durée de l'autorisation donnée par le juge ne peut être reporté au jour de la mise en place effective, par les officiers et agents de police judicaire, du système d'enregistrement sans qu'il soit directement porté atteinte à l'autorité et au contrôle effectif du juge d'instruction ; que l'arrêt attaqué encore violé les textes visés au moyen ;

« et aux motifs qu'il résulte du dossier que, les enquêteurs agissant sur commission rogatoire spéciale du juge d'instruction, ont fait procéder à la mise en place du dispositif de sonorisation le 20 avril 2007 lequel a été opérationnel le 23 avril ; qu'il a été mis fin, en accord avec le magistrat instructeur, à l'enregistrement des conversations le 20 juin 2007, date du départ en vacances de Serge L. et sa famille, sans prolongation du dispositif et sans désinstallation du matériel ; que, toutefois, les enquêteurs constatant que Serge L. faisait des allers et retours entre son lieu

de vacances et son domicile, sollicitaient la prolongation du dispositif de sonorisation ; que, sur réquisitions conformes, le juge d'instruction délivrait, le 5 juillet 2007, une ordonnance aux fins de prolongation du dispositif technique ; qu'aucune disposition légale n'impose le retrait du dispositif de sonorisation et de captation d'images ; que, dès lors, la captation autorisée pour une durée effective de deux mois à compter de l'installation du dispositif, le 20 avril 2007, ayant cessé le 20 juin 2007, aucun grief n'est fait aux droits des demandeurs en l'absence d'obligation de retrait d'un dispositif rendu inactif ; que, dès lors, l'ordonnance de prolongation et la commission rogatoire établies le 5 juillet 2007 sont régulières ;

« alors qu'aux termes de l'article 706-96 du Code de procédure pénale l'autorisation donnée par le juge porte sur la mise en place d'un dispositif technique d'enregistrement dans un lieu privé en sorte que la durée qui doit être obligatoirement mentionnée dans cette ordonnance selon l'article 706-97 du même code est celle du maintien en place de ce dispositif ; qu'en conséquence, à l'expiration de la durée fixée par le juge, en l'absence de renouvellement, le dispositif technique doit être retiré, avec, s'il est besoin d'opérer en dehors des heures légales, l'autorisation du juge des libertés et de la détention ; qu'en décidant que le dispositif pouvait être maintenu en place après l'expiration de la durée fixée par le juge d'instruction, l'arrêt attaqué a de nouveau méconnu le sens et la portée des textes précités ;

« alors que, d'autre part, le renouvellement de l'autorisation ne peut légalement intervenir qu'avant l'expiration de la durée initiale fixée par le juge ; que, dès lors, le juge d'instruction ne pouvait valablement renouveler le 5 juillet 2007 une autorisation qui avait pris fin au plus tard le 20 juin 2007 ;

« alors qu'enfin, selon l'article 706-101 seules peuvent être versées au dossier les conversations enregistrées qui sont utiles à la manifestation de la vérité ; que les dates et lieu de vacances de Serge L. et sa famille que les enquêteurs avaient appris par l'exploitation des sonorisations (PV D 121) n'étaient pas utiles à la manifestation de la vérité et ne pouvaient, en conséquence, ni apparaître dans la procédure ni être exploitées pour décider du maintien en place du dispositif de surveillance inactif » ;

Vu les articles 706-96, 706-97 et 706-98 du Code de procédure pénale ;

• Attendu qu'il résulte de ces textes que le renouvellement d'une autorisation de mise en place d'un dispositif technique ayant pour objet, sans le consentement des intéressés, la captation, la fixation, la transmission et l'enregistrement de paroles prononcées par une ou plusieurs personnes à titre privé ou confidentiel, dans des lieux ou véhicules privés ou publics, ou de l'image de personnes se trouvant dans un lieu privé, doit intervenir avant l'expiration de la mesure précédente ;

• Attendu qu'après avoir écarté l'argumentation des demandeurs qui soutenaient que le point de départ des mesures de sonorisation devait être fixé au jour du prononcé de la décision et non pas à partir de leur mise en place, l'arrêt a également rejeté le moyen de nullité pris de la tardiveté de la mesure de renouvellement prononcée après l'expiration de l'autorisation précédente ;

• Attendu qu'en cet état, la chambre de l'instruction a décidé à bon droit que le point de départ des mesures de sonorisation devait être fixé au jour de leur mise en place effective ;

• Mais attendu qu'en déclarant également régulière l'ordonnance de renouvellement intervenue le 5 juillet 2007 alors que l'autorisation précédente avait pris fin le 23 juin 2007, la chambre de l'instruction a méconnu les textes susvisés et le principe énoncé ci-dessus ;

• D'où il suit que la cassation est encourue de ce chef ;

[...]

Table des matières