

Commission nationale de contrôle des interceptions de sécurité

19^e rapport d'activité 2010

**Commission nationale de contrôle
des interceptions de sécurité**

35, rue Saint-Dominique
75007 Paris

Téléphone : 01 45 55 70 20

Télécopie : 01 45 55 71 15

Courriel : secretariat.cncis@pm.gouv.fr

« En application de la loi du 11 mars 1957 (article 41) et du Code de la propriété intellectuelle du 1^{er} juillet 1992, complétés par la loi du 3 janvier 1995, toute reproduction partielle ou totale à usage collectif de la présente publication est strictement interdite sans autorisation expresse de l'éditeur. Il est rappelé à cet égard que l'usage abusif et collectif de la photocopie met en danger l'équilibre économique des circuits du livre. »

Sommaire

Avant propos	5
Première partie	
RAPPORT D'ACTIVITÉ	7
Chapitre I	
Organisation et fonctionnement de la Commission	9
Chapitre II	
Le contrôle des interceptions de sécurité (loi n° 91-646 du 10 juillet 1991)	15
Chapitre III	
Le contrôle des opérations de communication des données techniques en matière de prévention du terrorisme (loi n° 2006-64 du 23 janvier 2006)	33
Deuxième partie	
JURISPRUDENCE DE LA COMMISSION.....	43
Troisième partie	
ÉTUDES ET DOCUMENTS	59
Chapitre I	
Présentation ordonnée des textes relatifs aux missions de la Commission	61
Chapitre II	
Interceptions de sécurité et secret-défense	89
Chapitre III	
Éléments de jurisprudence et actualités parlementaires.....	93
Table des matières	117

Avant propos

La CNCIS va entrer dans sa vingtième année.

Président de cette autorité administrative indépendante depuis plus d'un an, j'ai pu constater la très grande efficacité et l'utilité de cette Commission pour le contrôle des interceptions de sécurité, en particulier dans le domaine de la prévention de la délinquance et de la criminalité organisée qui est demeuré au cours de l'année 2010, le motif principal des demandes d'interception.

Contrairement à d'autres autorités indépendantes, la suppression de la CNCIS n'a jamais été envisagée. Celle-ci reste en effet un organe de contrôle spécifique non absorbable par une autre structure. Grâce à sa jurisprudence évolutive en fonction des nouveaux moyens techniques de communication, la CNCIS répond toujours aux attentes du législateur de 1991 avec le souci permanent de la recherche d'un équilibre entre la protection de la vie privée et les impératifs de la protection de la sécurité de la nation et des intérêts supérieurs de l'État.

Comme le souligne ce rapport concernant l'année 2010, le contrôle en aval des interceptions de sécurité s'est développé notamment par le suivi accru des « productions ». Par ailleurs, la politique de dialogue avec les services s'est intensifiée ce qui permet de mieux faire connaître la jurisprudence de la CNCIS.

Il convient, pour conclure cet avant-propos, de souligner que la composition de la CNCIS a, durant l'année 2010, été modifiée. Après le départ, vers le Conseil Constitutionnel, de M. Hubert HAENEL à qui je tiens à rendre hommage pour la mission qu'il a brillamment accomplie pendant plusieurs années au sein de cette commission. On ne peut que se réjouir de l'arrivée de M. le Sénateur Jean-Jacques HYEST, Président de la Commission des lois au Sénat. Son expérience nous est précieuse.

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 :

- Hervé PELLETIER, président de chambre à la Cour de Cassation, nommé pour une durée de 6 ans par le Président de la République – décret du 3 octobre 2009, publié au *Journal officiel* le 4 octobre 2009

- Jean-Jacques HYEST, membre parlementaire – Sénat : sénateur (UMP) de la Seine-et-Marne Île-de-France, désigné le 2 juin 2010 par le Président du Sénat, en remplaçant du sénateur HAENEL, nommé membre du conseil constitutionnel

- Daniel VAILLANT, membre parlementaire – Assemblée nationale : député (PS) de Paris, désigné le 1^{er} 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

- Olivier GUÉRIN, chargé de mission depuis sa nomination en date du 1^{er} juin 2010

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, 1^{er} octobre 1991
- Dieudonné MANDELKERN, président de section au Conseil d’État, 1^{er} octobre 1997
 - Jean-Louis DEWOST, président de section au Conseil d’État, 1^{er} 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, 1^{er} 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.

- Jean-Jacques HYEST nommé le 2 juin 2010 en remplacement du Sénateur Hubert HAENEL nommé membre du Conseil Constitutionnel.

Missions et fonctionnement

La Commission est chargée de veiller au respect des dispositions du titre II (« Des interceptions de sécurité ») de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, modifiée à plusieurs reprises, la dernière fois par la loi n° 2006-64 du 23 janvier 2006.

Conformément à l'article 1^{er} 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 ». Le président dispose d'une habilitation permanente à l'effet de formuler les avis dès lors que la demande d'interception ne pose pas de questions nouvelles par rapport à la jurisprudence établie.

En application de l'article 15 de la loi, la Commission reçoit les réclamations des particuliers, procède, en toute indépendance, aux contrôles et enquêtes qui lui paraissent nécessaires à l'accomplissement de sa mission et s'attache à nouer tous contacts utiles à son information.

Elle peut à tout moment adresser au Premier ministre une recommandation tendant à ce qu'une interception soit interrompue.

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

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

Enfin, elle est représentée par ses agents aux réunions de la Commission consultative créée par le décret n° 97-757 du 10 juillet 1997 qui, sous la présidence du 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 2010 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 2010 se sont élevés à 586 222 euros dont 502 475 euros pour les dépenses du titre II (dépenses de personnel) et à 83 747 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, deux secrétaires fonctionnant en binômes ainsi que d’un conducteur. 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 depuis 2009 d’importants travaux de rationalisation financière au sein desquels on peut, à titre d’exemple pour 2010, citer la finalisation d’une convention relative aux charges exposées, notamment au titre de l’occupation immobilière de la Commission, par la Direction des services administratifs et financiers du Premier Ministre et donnant lieu à la facturation vers la CNCIS.

Relations extérieures

Au mois d’avril 2010 et dans le prolongement des échanges avec les autorités Bulgares déjà évoqués dans le rapport d’activité de 2009, la Commission a poursuivi ces travaux à la faveur d’une visite en ses locaux

d'une Délégation composée notamment du Vice – ministre de l'Intérieur bulgare et du Directeur du cabinet du Ministère de l'Intérieur bulgare.

De même, au mois de septembre 2010, la Commission a reçu la visite d'une délégation représentant le G10 allemand, celui-ci constituant, sous une forme et un périmètre de mission juridiquement différents du régime français, l'autorité de contrôle des interceptions de sécurité pratiquées en Allemagne.

Chapitre II

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

Le contrôle des autorisations

Il convient ici de décrire la nature et la portée du contrôle pratiqué par la Commission sur les demandes d'interception dont elle est saisie.

Ce contrôle peut être qualifié de spectral en ce qu'il intervient tant en amont de l'autorisation d'interception qui relève du pouvoir exclusif du Premier ministre (article 4 de la loi du 10 juillet 1991) qu'en aval de cette décision et qu'il porte tant sur la forme que sur le fond de la demande d'interception.

Des éléments d'actualité ont, au mois de septembre 2010, conduit la Commission à clarifier et préciser le périmètre de ce contrôle par un communiqué de presse en date du 30 septembre 2010.

- Une clarification quant à la limite de son pouvoir de contrôle résultant de l'article 20 de la loi du 10 juillet 1991 :

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. »

Par cet article, le législateur a entendu réserver une exception au principe du contrôle des seules interceptions de sécurité par la CNCIS, qui trouve sa source dans la nature même des mesures concernées, à savoir une surveillance générale du domaine radio – électrique, par des opérations aléatoires de balayage des fréquences.

On relève, notamment dans les travaux préparatoires du texte précité, que « *ces techniques réalisées dans le cadre de la mission générale de défense et ne visant pas de communications individualisables ne peuvent être considérées comme des ingérences de l’autorité publique dans l’exercice par toute personne de son droit au respect de sa correspondance au sens de l’article 8 de la CEDH* ».

Au sujet de ce dispositif et au regard de la problématique particulière de l’interception des communications passées à partir des téléphones portables qui n’utilisent que la voie hertzienne, la Commission, dès 1998 (rapport 98 p. 36) indiquait clairement que l’évolution technologique ne pouvait occulter le but poursuivi par le législateur en 1991, c’est-à-dire la protection du secret de la correspondance en son principe, sans en résumer le support à « l’existant technologique » ou à sa possible évolution.

En quelques lignes contenues dans son rapport d’activité, la Commission rappelait ainsi la primauté du principe de libertés publiques sur l’évolution technique en indiquant que l’exception à son contrôle prévue par l’article 20 devait s’interpréter strictement :

« Toute interception de correspondance échangée par la voie des télécommunications, qui n’entre pas dans le champ de l’article 20, est soumise quel que soit le mode de transmission filaire ou hertzien aux conditions et aux procédures fixées par la loi du 10 juillet 1991 ».

Cette règle a, depuis cette date, été régulièrement rappelée dans les décisions prises par la Commission, notamment pour définir les modalités de son contrôle en matière de recueil des données techniques des communications dans le champ de la loi du 10 juillet 1991.

- Une précision quant à « l’étendue technique » de son contrôle sur l’interception de sécurité.

Cette précision fût ainsi l’occasion de revenir sur une distinction déjà opérée par la Commission à partir de l’observation du « socle unique » de la communication. Deux éléments distincts constituent en effet les pièces indissociables de ce socle :

- le contenu de la communication (échange de paroles, de messages, de signes...);
- le contenant de cette même communication constitué de l’agrégat de données techniques formant l’accessoire co-substantiel de la communication et qui permettent tant d’en attester l’existence que d’en définir le contexte. Il s’agit pour l’essentiel des données d’identification, de facturation détaillée (fadets) ou de localisation géographique des équipements utilisés pour la communication.

Ces données sont devenues, au fil des ans, un élément opérationnel incontournable pour les services de renseignement ou de police judiciaire.

Pour ce qui concerne la Commission quant au contrôle qu'elle exerce sur ce type de données, il y a lieu d'observer deux fondements juridiquement distincts :

- l'article 6 de la loi du 23 janvier 2006 qui encadre comme nous le détaillerons plus avant dans ce rapport (p. 34), l'accès à ce type de mesure pour la seule prévention des actes de terrorisme à travers une procédure spécifique. Ce dispositif est totalement détaché de la notion d'interception de sécurité.
- l'article 22 de la loi du 10 juillet 1991 : ces données sont, par la rédaction même de cet article intrinsèquement rattachées à la notion d'interception de sécurité. Elles sont soumises à une procédure particulière de contrôle.

Article 22 – (modifié par l'article 18 de la loi n° 96-659 du 26 juillet 1996 sur la réglementation des télécommunications) – « Les juridictions compétentes pour ordonner des interceptions en application du Code de procédure pénale ainsi que le Premier ministre ou, en ce qui concerne l'exécution des mesures prévues à l'article 20, le ministre de la Défense ou le ministre de l'Intérieur, peuvent recueillir, auprès des personnes physiques ou morales exploitant des réseaux de "communications électroniques" ou fournisseurs de services de "communications électroniques", les informations ou documents qui leur sont nécessaires, chacun en ce qui le concerne, pour la réalisation et l'exploitation des interceptions autorisées par la loi.

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

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

La CNCIS a, sur le fondement des dispositions de cet article, défini une procédure de contrôle reposant sur les principes suivants :

- la centralisation, le traitement et le contrôle a priori des demandes des services par le groupe interministériel de contrôle relevant du premier ministre;
- le contrôle a posteriori hebdomadaire de ces demandes par la CNCIS;
- la possibilité pour la Commission, de recourir aux mêmes avis et recommandations que ceux adressés au Premier ministre, dans le cadre des interceptions de sécurité.

Au terme de délibérations successives conduites en 2009 et 2010 dans sa formation plénière, la CNCIS a, en outre, soumis ce dispositif à une évaluation générale annuelle.

Elle a, enfin, rappelé l’interdiction faite aux services de solliciter directement les opérateurs pour les demandes de prestations relevant de la compétence de la Commission.

Le contrôle en amont

Théorie et pratique du contrôle

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

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

Enfin, le président de la Commission est informé par le GIC des décisions prises par le Premier ministre ou les personnes déléguées par celui-ci dans les conditions prévues par la loi de 1991. En cas de désaccord, il soumet la divergence d’appréciation à la délibération de la Commission conformément à l’article 14 de la loi. Dans l’hypothèse où le désaccord est confirmé, une recommandation tendant à l’interruption de l’interception en cause est adressée au Premier ministre. Il convient toutefois de noter que depuis la transmission pour avis *a priori* de l’intégralité des demandes d’interception, cette disposition a perdu son intérêt sauf bien sûr pour ce qui concerne les interceptions déjà en cours et dont la Commission recommande au Premier ministre de décider de les interrompre, ou préconise directement aux services cette interruption.

Contrôle formel et respect des contingents

L’activité de contrôle comporte, en premier lieu, un aspect formel qui consiste à vérifier que les signataires des demandes d’autorisation ont bien été habilités par les ministres compétents. Devant la multiplication des demandes urgentes et afin de fluidifier les procédures, la Commission a suggéré et obtenu que la loi n° 2006-64 du 23 janvier 2006

introduise à l'article 4 de la loi du 10 juillet 1991 une nouvelle disposition autorisant chaque ministre, à l'instar du Premier ministre, à déléguer de façon permanente sa signature à deux personnes.

Il convient de rappeler que les contingents d'interceptions simultanées ne doivent pas être confondus avec le nombre total d'interceptions (demandes initiales et renouvellements) réalisées annuellement au profit des trois ministères concernés, Intérieur, Défense et Budget. Dans son souci de conserver un caractère exceptionnel aux interceptions de sécurité, le législateur de 1991 a en effet opté pour une limitation sous forme d'un encours maximum, protecteur des libertés publiques. Ce système déjà mis en place par la décision du 28 mars 1960 du Premier ministre Michel Debré, mais résultant à l'époque de contraintes techniques (capacité maximale d'enregistrement sur des magnétophones à bandes ou à cassettes et capacité d'exploitation par le GIC) a été consacré en 1991 comme devant « inciter les services concernés à supprimer le plus rapidement possible les interceptions devenues inutiles, avant de pouvoir procéder à de nouvelles écoutes » (CNCIS, 3^e 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 réservier 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), qui sont 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, depuis 2009, du sous contingent de la gendarmerie nationale au sein du contingent du Ministère de l'intérieur.

L'année 2010 a été marquée par le deuxième exercice de l'interprétation par la Commission de ce contingent comme se référant à un nombre maximum de « cibles » et non plus de « lignes ». 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 sont, 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, ainsi que 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 de contrôler 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 à 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 celles 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 les activités jugées sensibles en raison du rôle qu’elles jouent dans une société démocratique. Il importe aussi de s’assurer que le motif légal invoqué ne dissimule pas d’autres préoccupations. Il est nécessaire de rappeler que l’interception doit être sollicitée exclusivement pour les faits articulés et non pour une raison autre qui ne relèverait d aucun motif légal, quelle que soit par ailleurs la véracité des faits rapportés. 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'ils ne tombent pas sous le coup de la loi, ne justifient pas en tant que tels une demande d'interception s'ils ne comportent aucune menace immédiate pour l'ordre public républicain, matérialisée par exemple par un appel ou un encouragement à la violence. De même, elle veille à ce que les interceptions, en ce qu'elles sont parfois concomitantes d'actions sur le terrain, ne portent pas atteinte à la liberté de manifestation.

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

Le président de la CNCIS peut demander les éléments d'informations complémentaires qui lui sont nécessaires pour fonder l'avis de la Commission. Il formule également les observations qu'il juge utiles sur la pertinence du motif invoqué, procédant le cas échéant à des propositions de substitution de motif.

Il s'assure que la demande respecte le **principe de proportionnalité** entre le but recherché et la mesure sollicitée. La gravité du risque ou du danger pour la sécurité des personnes, qu'elles soient physiques ou morales, ou pour la sécurité collective, doit être à la mesure de l'atteinte à la vie privée que constitue la surveillance de la correspondance par voie de communications électroniques, et justifier cette atteinte. La recherche de cette proportionnalité peut se traduire *ab initio* ou lors du renouvellement par une restriction au cas par cas de la durée de la mesure dont le maximum est de quatre mois. Une différenciation des délais a été instaurée par voie jurisprudentielle : deux mois pour une cible non totalement identifiée, délai *ad hoc* calé sur un événement prévu à date fixe, etc.

On peut également citer 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.).

Données chiffrées et commentaires

- Évolutions 2009-2010

6010 interceptions de sécurité ont été sollicitées en 2010 (3776 interceptions initiales et 2234 renouvellements).

S'agissant des interceptions initiales, 522 de ces 3776 demandes ont été présentées selon la procédure dite d'urgence absolue (497 en

2009) soit 13,2 % de ces demandes (18,9 % en 2009). Cette diminution constante du pourcentage d’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 a 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 31 avis négatifs donnés par la Commission lors des demandes initiales et des demandes de renouvellement, tous suivis par le Premier ministre, ce sont donc 5 979 interceptions de sécurité qui ont effectivement été pratiquées au cours de l’année 2010 (5 029 en 2009).

Pour ce qui concerne les motifs au stade des demandes initiales, la prévention de la criminalité et de la délinquance organisées reste le premier motif des demandes initiales avec 62,6 %, suivie de la prévention du terrorisme avec 20 % et la sécurité nationale 16,6 %.

Concernant les renouvellements, on note que la sécurité nationale occupe la première place avec 42,1 % suivie de la prévention du terrorisme 30,6 % et de la criminalité organisée 25,6 %. 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 48,8 % suivie de la sécurité nationale 26,1 % et puis la prévention du terrorisme 24 %. Ces trois motifs représentent quasiment 99 % du total des demandes.

- Observations

La Commission a poursuivi sa démarche de dialogue avec les services demandeurs. Cette démarche s'est traduite par une nette augmentation des réunions bilatérales avec ces mêmes services. Elle s'est également matérialisée, au stade de l'examen de leurs demandes, par une logique d'avis moins binaire (avis favorable/défavorable). De fait, le nombre d'observations a encore crû, passant de 1 651 en 2009 à 2 101 en 2010 dont 79 demandes de renseignements complémentaires et 487 limitations de la durée d'interception sollicitée. Les avis défavorables comptabilisés dans les observations se sont élevés à 31, se répartissant à

17 concernant les demandes initiales et 14 pour les demandes de renouvellement. Tous ces avis négatifs ont été suivis 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 7 reprises en 2010. 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 » 57 interceptions en 2010.

De fait, si l'on additionne avis négatifs, recommandations d'interruption adressées au Premier ministre et « préconisations d'interruption » formulées 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 2010 à 95.

Le contrôle en aval

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 rendre 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 560 interceptions en 2010 (326 en 2009) 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. 4 de ces recommandations ont été ainsi adressées au Premier ministre au cours de l'année 2010.

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 5 979 interceptions accordées en 2010, on constate cette année encore, que les interceptions de sécurité demeurent, au regard de vecteurs de communications électroniques en constante augmentation, la mesure d'exception voulue par la loi.

Tableaux annexes

Les demandes initiales d'interception

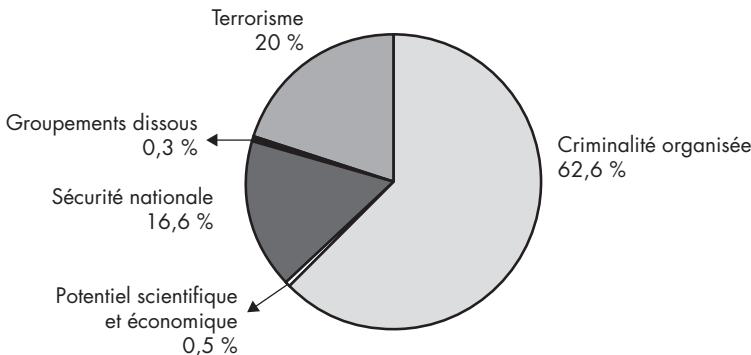
État des demandes initiales d'interception (2009 et 2010)

	Demandes initiales		Dont urgence absolue		Accordées	
	2009	2010	2009	2010	2009	2010
Totaux	3 176	3 776	497	522	3 113	3 759

Demandes initiales

Répartition des motifs

2010

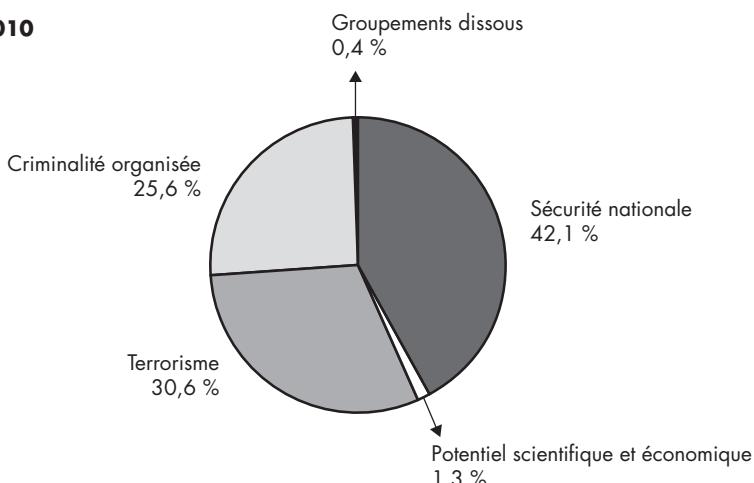


Les renouvellements d'interception

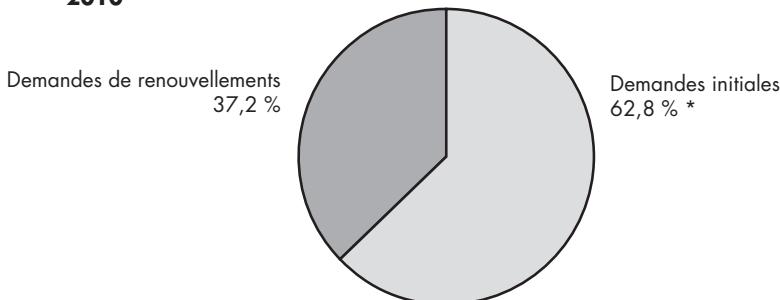
Total des renouvellements demandés : 2 234

Répartition des motifs des renouvellements accordés en 2010

Sécurité nationale	Potentiel scientifique et économique	Terrorisme	Criminalité organisée	Groupements dissous	Total «accordés»
935	28	680	569	8	2 220

2010**Activité globale : demandes initiales et renouvellements****Répartition des demandes entre interceptions et renouvellements d'interceptions**

Demandes initiales circuit normal		Demandes initiales en urgence absolue		Demande de renouvellement	
2009	2010	2009	2010	2009	2010
2 616	3 254	497	522	1 916	2 234

2010

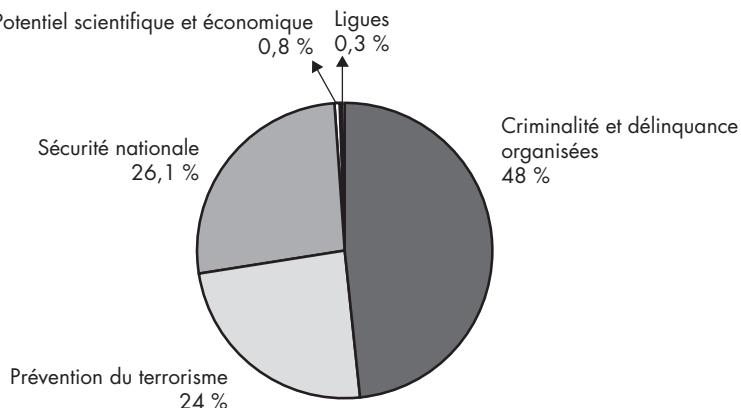
* Rappel : 13,2 % des demandes initiales sont constituées par des demandes présentées en urgence absolue.

Demandes d'interceptions : tableau récapitulatif global sur cinq ans

	2006	2007	2008	2009	2010
Demandes initiales d'interceptions	4 203	4 215	4 330	3 176	3 776
Dont «urgence absolue»	714	964	1 095	497	522
Demandes de renouvellements	1 825	1 850	1 605	1 941	2 234
Total	6 028	6 065	5 935	5 117	6 010

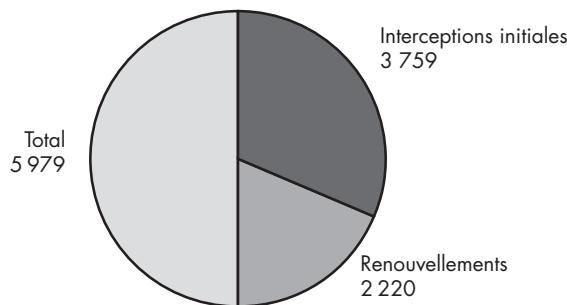
Répartitions des motifs d'interceptions de sécurité accordées :

Cumul des demandes initiales et des demandes de renouvellements accordés



Répartition entre interceptions et renouvellements accordés

Interceptions accordées en 2010



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 1300/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, 11^e 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

Durant l’année 2010, 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, 17 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 des procédures mises en œuvre par les services pour l’application de la loi du 10 juillet 1991. Ils apportent les informations et les 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, 48 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 nombre d’appels téléphoniques bien supérieur à celui des saisines par courrier. Ces contacts préalables ont le plus souvent permis de prévenir des requêtes ultérieures mal fondées ou mal orientées lorsqu’il s’agit par exemple 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] puis de 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 1^{er} du projet de loi par une personne privée;
- absence de toute interception.

On comprendra aisément au vu de ces différentes hypothèses que la Commission nationale n'a d'autre possibilité que d'adresser la même notification à l'auteur d'une réclamation, quelle que soit la situation révélée par les opérations de contrôle, et que toute autre disposition conduirait, directement ou indirectement, la Commission à divulguer des informations par nature confidentielles (Assemblée nationale, rapport n° 2088 de François MASSOT, 6 juin 1991).

Faut-il en conclure que toute requête est inutile? Non, car même si le secret-défense interdit toute révélation sur l'existence ou l'inexistence d'une interception de sécurité, la CNCIS dispose de deux moyens d'action lorsqu'elle constate une anomalie :

- le pouvoir d'adresser au Premier ministre une recommandation tendant à faire interrompre une interception qui s'avérerait mal fondée;
- le pouvoir, qui est aussi un devoir, de dénonciation à l'autorité judiciaire de toute infraction à la loi de 1991 qui pourrait être révélée à l'occasion de ce contrôle (*cf. infra*).

Pour être complet signalons que :

- la Commission d'accès aux documents administratifs (CADA) arguant du secret-défense a émis le 18 décembre 1998 un avis défavorable à la demande de communication d'une copie d'une autorisation du Premier ministre concernant l'interception des communications téléphoniques d'un requérant;
- le Conseil d'Etat, 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 2010, la CNCIS n’a pas eu à user des dispositions du 2^e 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 par le décret 2009-834 du 7 juillet 2009 puis le décret 2009-1657 du 24 décembre 2009. Depuis, la présidence de cette Commission est confiée 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.

Le 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 n° 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 cinq fois en 2010. 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 2010, la Commission a rendu 643 décisions ventilées comme suit :

- 321 décisions d'autorisation initiale (236 concernant la commercialisation, 85 l'acquisition d'équipements soumis à autorisation);
- 110 décisions de renouvellement d'autorisation;
- 163 décisions d'ajournement;
- 13 décisions de refus ou de retrait;
- 15 décisions de mise « hors champ » de l'examen pour autorisation;
- 21 décisions de radiations.

À la différence des années précédentes (*cf. rapports 2005 à 2009*) il est observé une diminution importante du nombre de décisions de mise « hors champ » de l'examen de la Commission. Cette évolution résulte vraisemblablement d'une meilleure connaissance des dispositions de l'arrêté du 29 juillet 2004, qui emportent l'exclusion de certains types de matériels, qui étaient jusqu'à cette date soumis à autorisation.

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

Ces services 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 visites 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 en matière de prévention du terrorisme (loi n° 2006-64 du 23 janvier 2006)

L'année 2010 constitue le troisième exercice annuel complet de l'activité du dispositif de prévention du terrorisme mis en œuvre sur le fondement de l'article 6 de la loi du 23 janvier 2006 inséré à l'article L. 34-1-1 du code des postes et des communications électroniques.

Ces dispositions prévoient qu'*« afin de prévenir 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 des personnes mentionnées au I de l'article L. 34-1 la communication des données conservées et traitées par ces derniers en application dudit article. »*

Tirant les enseignements des attentats de Madrid du 11 mars 2004 et de Londres du 7 juillet 2005, soucieux d'assurer au mieux la sécurité de nos concitoyens alors que la menace terroriste pesait aussi sur la France, le législateur a autorisé les services de police et de gendarmerie spécialisés dans la prévention du terrorisme à se faire communiquer, sur le fondement d'une réquisition administrative spécifique, comparable à celle prévue par le code de procédure pénale, certaines données techniques détenues par les opérateurs de communications électroniques (OCE) et par les fournisseurs d'accès à Internet (FAI).

Le législateur a adopté un dispositif original dans l’ensemble des systèmes européens de contrôle des accès légaux aux communications électroniques, nécessaires pour garantir le respect des libertés publiques et la protection de la vie privée. La loi du 23 janvier 2006 institue ainsi une personnalité qualifiée auprès du ministre de l’Intérieur, relevant de la Commission nationale de contrôle des interceptions de sécurité pour son activité de contrôle de la légalité de l’action des services habilités en matière de prévention du terrorisme.

Ce dispositif, défini dans la loi du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, a été prévu à titre expérimental dans un premier temps jusqu’au 31 décembre 2008. Il a été prorogé jusqu’au 31 décembre 2012 par la loi n° 2008-1245 du 1^{er} décembre 2008.

Ainsi, année médiane de la période d’expérimentation fixée par le législateur, l’année 2010 constitue une étape nouvelle et importante pour l’évaluation de ce dispositif dans un contexte très renouvelé tant sur le plan des menaces terroristes, qu’au niveau des besoins opérationnels des services judiciaires et de renseignement apparus pour s’adapter à ces nouvelles formes d’actions terroristes. Les dispositifs juridiques internes, européens et internationaux dans le domaine de la lutte contre le terrorisme sont aussi en pleine évolution.

Les responsabilités attachées aux fonctions de la « personnalité qualifiée » sont confiées depuis le 27 novembre 2009 au contrôleur général Jean ESPITALIER. Que cette partie du rapport d’activité soit l’occasion de le remercier publiquement pour l’action qu’il conduit avec le souci constant de traiter dans les meilleures conditions d’efficacité et de célérité les demandes des services engagés dans la lutte contre le terrorisme, tout en garantissant la protection des libertés publiques et des droits individuels que le législateur a entendu préserver.

Par son travail et son sens constant du dialogue, il a su instaurer avec les services une démarche de collaboration fructueuse dans le respect des contraintes de chacun et des objectifs définis par le législateur.

Il a su maintenir et enrichir les conditions d’un dialogue constructif avec la Commission nationale de contrôle des interceptions de sécurité, en charge du contrôle a posteriori des demandes validées par les services de la « personnalité qualifiée ». Il veille avec une attention particulière à l’adoption de solutions jurisprudentielles conformes à celles développées par la Commission nationale de contrôle des interceptions de sécurité, dans les autres secteurs plus anciens du contrôle de l’exploitation des communications électroniques, relevant de la compétence de cette dernière. Cette préoccupation constante est une condition essentielle de l’efficacité de l’action des services et de la protection des garanties des droits des personnes voulue par le législateur.

Ces observations et ces remerciements s'adressent aussi aux adjoints de la personnalité qualifiée dont deux d'entre eux ont été reconduits dans leur fonction par décision de la CNCIS au cours de l'année 2010.

Présentation du dispositif

Les agents individuellement désignés et dûment habilités pour conduire les investigations au titre de l'article 6 relèvent de six services de la police nationale et de la gendarmerie nationale, chargés de la prévention du terrorisme. Il s'agit de :

- la direction centrale du renseignement intérieur (DCRI),
- la direction du renseignement de la préfecture de police (DRPP),
- la direction centrale de la police judiciaire (DCPJ),
- la direction régionale de police judiciaire de Paris (DRPJ – Paris),
- l'unité de liaison et de coordination de la lutte anti-terroriste (l'UCLAT),
- la direction générale de la gendarmerie nationale – bureau de liaison anti – terroriste (BLAT).

En 2010, il est constaté une hausse du nombre global de ces « agents individuellement désignés et dûment habilités » de près de 25 % par rapport à l'année précédente. L'augmentation des effectifs de la DCRI est la plus importante, soit plus de 29 %. Ces personnels représentent désormais 76,33 % de l'ensemble.

Les services en charge de missions de renseignement et l'UCLAT représentent 79,64 % de l'effectif total, alors que la part des personnels relevant des unités à compétence judiciaire est de 20,36 %.

	État des effectifs au 31.12.2008	État des effectifs au 31.12.2009	État des effectifs au 31.12.2010
UCLAT	15	13	13
DCRI	457	499	645
DRPP	10	21	15
DCPJ	77	77	92
DRPJ PARIS	58	46	62
DGGN BLAT	24	20	18
Total	641	676	845

La possibilité pour les services de l'État d'obtenir sur réquisition administrative les données techniques afférentes à une communication électronique, c'est-à-dire d'avoir accès au « contenant » de celle-ci (identification des numéros appelés ou appelants, détail des contacts, géolocalisation des terminaux utilisés) sans pouvoir en obtenir « le contenu », tel que l'échange des correspondances et les conversations, constitue un outil important de recueil de renseignements techniques en matière de prévention du terrorisme.

Ces mesures sont moins intrusives dans la vie privée et moins attentatoires sur le plan des libertés publiques que l’interception des communications qui permet d’appréhender le contenu des échanges et des conversations. Néanmoins, elles portent atteinte partiellement au droit à l’intimité de la vie privée et au secret des correspondances.

En ce sens, les instances européennes et nationales ont toujours admis le principe d’une atteinte par la puissance publique, fondée sur des motifs supérieurs de sécurité nationale et des personnes, notamment dans le cadre de la prévention et de la lutte contre les infractions les plus graves portant atteinte à la vie humaine et aux intérêts fondamentaux de la Nation, comme les actes terroristes.

Dans ce but, les mesures de renseignement technique fournies par l’article 6 de la loi du 23 janvier 2006 permettent d’écartier ou de confirmer par des premières vérifications simples et rapides, les informations ouvertes et publiques, celles recueillies auprès de sources humaines variées (institutionnelles, internes ou étrangères, particuliers), et les données techniques brutes.

Les recherches effectuées sur le fondement de l’article 6 sont à même de fournir des éléments matériels ou des indices susceptibles de conforter des présomptions d’implication ou de projets terroristes. Dans cette hypothèse, elles sont indispensables à l’ouverture d’une enquête judiciaire.

Ces mesures constituent un complément essentiel pour étayer les hypothèses d’enquête et les renseignements collectés, en dehors de procédures judiciaires, afin de conforter les éléments ou les indices probants sur des projets et des préparations d’attentats, en amont de leur perpétration. Compte tenu de la particulière gravité et de la dangerosité exceptionnelle du terrorisme, la prévention de ces actions et la neutralisation des auteurs constituent un objectif essentiel avant le passage à l’acte.

Éléments d’ordre statistique

Pour les trois années, de 2008 à 2010, les demandes des services traitées par la « personnalité qualifiée » se décomposent de la façon suivante :

	Demandes présentées	Demandes validées	Demandes renvoyées	Demandes rejetées
2008	38 306	34 911	3 302	93
2009	43 559	39 070	4 459	30
2010	45 716	38 566	7 060	90
Total	127 581	112 547	14 821	213

Au cours de ces trois années, soit 157 semaines, si en moyenne 813 demandes ont été traitées chaque semaine par la personnalité qualifiée, en réalité on observe une progression annuelle des demandes formulées par les services : 737 en 2008, 822 en 2009 et 879 en 2010, année de la plus forte activité de la « personnalité qualifiée » depuis sa création.

	Période 2008/2009	2008 (52 semaines)	2009 (53 semaines)	2010 (52 semaines)
Demandes présentées	812,7	736,7	821,9	879,2
Demandes validées	716,9	671,4	737,2	741,7
Demandes renvoyées	94,4	63,5	84,1	135,8
Demandes rejetées	1,4	1,8	0,6	1,7

	Demandes présentées	Demandes validées	Demandes renvoyées	Demandes rejetées
2008/2010	+ 7410 (+ 19,34 %)	+ 3 655 (+ 10,47 %)	+ 3 758 (+ 113,80 %)	- 3 (- 3,23 %)
2008/2009	+ 5 253 (+ 13,71 %)	+ 4 159 (+ 11,91 %)	+ 1 157 (+ 35,04 %)	- 63 (- 67,74 %)
2009/2010	+ 2 157 (+ 4,96 %)	- 504 (- 1,29 %)	+ 2 601 (+ 58,33 %)	+ 60 (+ 200 %)

Il résulte de ces données statistiques que :

- le nombre des demandes présentées a augmenté de 19,34 % entre 2008 et 2010 avec une hausse de 13,71 % entre 2008 et 2009 et de 4,96 % entre 2009 et 2010, caractérisant ainsi un tassement relatif de l'accroissement en 2010, même si l'activité est à son niveau le plus élevé ;
- en valeur absolue, les demandes validées ont suivi la même hausse. Néanmoins, il est constaté une baisse annuelle du taux de validation des demandes, tendance accentuée en 2010. Ainsi en 2008, ce taux était de 91,14 %, alors qu'en 2009 il est passé à 89,69 %, pour être de 84,36 % en 2010 ;
- le nombre des demandes renvoyées, afin d'obtenir des renseignements complémentaires sur les circonstances et les motifs des demandes présentées, a augmenté de + 11,61 % sur l'ensemble de la période avec une tendance à la hausse, soit un taux de renvoi de 8,62 % en 2008, de 10,23 % en 2009 et de 15,44 % en 2010. Le nombre hebdomadaire des demandes renvoyées a ainsi augmenté chaque année, avec une tendance accrue pour l'exercice 2009-2010 où le taux de renvoi a cru de 61,47 % alors qu'il n'était que de 32,44 % entre 2008 et 2009 ;
- le nombre des demandes définitivement rejetées n'a pratiquement pas évolué et est resté à un niveau faible. Représentant 0,24 % de l'ensemble des demandes présentées, il est passé à 0,07 % en 2009 pour remonter à 0,20 % en 2010.

Il convient de préciser que le chiffre des demandes validées ne correspond pas au nombre réel de « cibles » concernées. Il est très fréquent que plusieurs dizaines de demandes portant sur des mesures différentes

ou adressées à des opérateurs distincts concernent une même personne soupçonnée de menées terroristes.

L'étude par direction requérante du nombre des demandes validées confirme la tendance à la hausse en 2009 (+ 11,91 %), suivie en 2010 d'une baisse globale des résultats par rapport à l'année précédente (- 1,29 %) essentiellement en raison de la diminution des demandes formulées par les services à compétence exclusivement judiciaire :

	2008	2009	2010	Variation 2008/2009	Variation 2009/2010
DCRI	31 003	34 387	34 479	+ 3 384 (+ 10,92 %)	+ 92 (+ 2,68 %)
DRPP	2 562	3 093	2 576	+ 531 (+ 20,73 %)	- 517 (- 16,72 %)
DGGN	1 042	1 013	1 192	- 29 (- 2,78 %)	+ 179 (+ 16,67 %)
DCPJ	223	545	305	+ 322 (+ 144,39 %)	- 240 (- 44,03 %)
DRPJ-PARIS	73	25	12	- 48 (- 65,75 %)	- 13 (- 52 %)
UCLAT	8	7	2		
Total	34 911	39 070	38 566	+ 4 159 (+ 11,91 %)	- 504 (- 1,29 %)

Dans le même temps, le nombre des demandes renvoyées pour renseignements complémentaires a connu une hausse constante témoignant d'un contrôle a priori de la légalité par la « personnalité qualifiée » plus exigeant, au fur et à mesure de l'augmentation croissante des services et des personnels habilités ainsi que des demandes formulées.

	2008	2009	2010	Variation 2008/2009	Variation 2009/2010
DCRI	3 032	4 180	6 719	+ 1 148 (+ 37,86 %)	+ 2 539 (+ 60,74 %)
DRPP	96	106	123	+ 10 (+ 10,42 %)	+ 17 (+ 16,04 %)
DGGN	98	115	136	+ 17 (+ 17,35 %)	+ 21 (+ 18,26 %)
DCPJ	61	47	71	- 14 (- 22,95 %)	+ 24 (+ 51,06 %)
DRPJ-PARIS	14	9	10		
UCLAT	1	2	1		
Total	3 302	4 459	7 060	+ 1 157 (+ 35,04 %)	+ 2 601 (+ 58,33 %)

Les données statistiques sur la nature des technologies, objet des demandes, permettent de constater que :

- la téléphonie mobile reste la technologie générant le plus de demandes ;
- les demandes concernant la téléphonie fixe progressent de manière constante, avec en 2010 une hausse de près de 23 % par rapport à 2009 ;

- inversement, les demandes de prestation Internet ont connu en 2010 une baisse significative.

Ces évolutions sont peut-être à rapprocher du succès croissant des offres commerciales «Triple Play», et bientôt «Quadruple Play», grâce auxquelles les particuliers ont désormais accès sous le même numéro d'abonnement à la téléphonie fixe, à Internet, et à de la téléphonie mobile, ainsi qu'à la télévision numérique.

	2008	2009	2010	Variation 2009/2010
Téléphonie mobile	31 446	30 509	31 129	+ 625 (+ 2,05 %)
Téléphonie fixe	5 289	7 824	9 609	+ 1 785 (+ 22,81 %)
Internet	1 571	5 231	4 971	- 260 (- 4,97 %)

Concernant la nature des prestations sollicitées par les services, 72,18 % portent sur des demandes d'identification, alors que 27,57 % couvrent les mesures liées au trafic.

Année 2010	Identification de l'abonné	Trafic de l'abonné
Téléphonie mobile	74,25 %	25,37 %
Téléphonie fixe	57,50 %	42,45 %
Internet	75 %	7,25 %

La typologie des demandes formulées par les services montre que la majeure partie d'entre elles, 72,18 % sont les mesures d'investigation les moins attentatoires à la vie privée, l'identification correspondant de manière concrète à la consultation facilitée d'un annuaire téléphonique.

Le traitement des demandes présentées au cours de l'année écoulée témoigne du souci constant de privilégier un dialogue constructif avec les services demandeurs en sortant de la logique binaire acceptation/refus pour privilégier en cas de difficultés, des renseignements complémentaires avant validation ou refus.

Les motifs des demandes de renseignements complémentaires résultent pour l'essentiel d'une motivation insuffisante sur les présomptions d'implication personnelle dans des menées à caractère terroriste, relatives à la personne objet de l'investigation. Parfois, elles peuvent tenir au non-respect des principes de proportionnalité et/ou de subsidiarité, quelques fois à la contradiction de motifs au sein de la demande, et dans quelques hypothèses à l'absence de précisions sur le mouvement d'appartenance de la cible.

Les motifs des refus définitifs des requêtes sont principalement liés à :

- des faits déjà commis et/ou faisant l'objet d'enquêtes judiciaires,
- des personnes dont les situations pénales ne permettent pas le recours à des mesures administratives,

- des faits insusceptibles en l’état de constituer des infractions revêtant une qualification en lien avec le terrorisme, en vertu des définitions des conventions internationales et européennes ainsi que du code pénal français.

Étendue et modalités du contrôle exercé par la CNCIS

De manière constante et générale, il a toujours été posé en application des principes démocratiques d’un État de droit, que les mesures d’investigation sur les communications électroniques doivent être explicitement prévues par la loi, qui doit préciser les motifs autorisant leurs recours et les conditions de leurs mises en œuvre.

Les instances européennes ont régulièrement rappelé dans leurs travaux et leurs décisions l’obligation de légiférer sur ces matières, en raison des impératifs d’information et de prévisibilité pour les citoyens, qui sont susceptibles d’être l’objet de ces mesures intrusives dans leur vie privée.

Les législations nationales doivent prévoir un contrôle des actions conduites dans cette matière par la puissance publique prérogative exercée par une autorité, dont la nature et la composition doivent garantir son indépendance, selon les instances exécutives parlementaires et juridictionnelles européennes.

Bien que moins intrusives que les interceptions de sécurité dans le secret des correspondances, les prestations entrant dans le champ de l’article 6 de la loi du 23 janvier 2006 sont cependant attentatoires et ne sont autorisées par le législateur que pour le seul motif de la prévention du terrorisme.

S’agissant d’un dispositif de nature administrative, à vocation préventive, utilisé par les services de renseignements, le législateur a souhaité l’encadrer de manière stricte en prévoyant des garanties pour le respect des droits des personnes, dont la protection est confiée à la « personnalité qualifiée » nommée par la CNCIS, et à celle-ci.

La première autorité assure un contrôle de la légalité a priori de l’ensemble des demandes de prestations des services. Ainsi, il n’est donné aucune suite à une requête qui ne serait pas validée par elle. La seconde a pour mission le contrôle de la légalité a posteriori des demandes validées par la « personnalité qualifiée ».

Ce double contrôle de la légalité s’exerce pour chaque demande des services sur les points suivants :

- des mesures sollicitées exclusivement par des « agents individuellement désignés et dûment habilités » ;

- des requêtes dûment motivées, et ce au regard de la seule prévention du terrorisme;
- des demandes ayant une vocation exclusivement préventive, en amont de toute enquête judiciaire,
- l’implication présumée, directe et personnelle, de la personne dans des menées terroristes,
- la proportionnalité entre le but recherché et la prestation sollicitée, appréciée en fonction de la gravité de la situation,
- la subsidiarité du recours à l’article 6, signifiant que le but recherché ne puisse être obtenu par d’autres moyens.

En application de ces principes, des demandes ont été définitivement rejetées en ce que les vérifications effectuées montraient que les mesures sollicitées relevaient d’investigations judiciaires, ou que les objectifs recherchés ne portaient pas sur des faits susceptibles de recevoir la qualification de terrorisme, mais plutôt d’atteintes à la sécurité nationale ou d’actes relevant de la criminalité et de la délinquance organisées.

Les demandes ont été renvoyées pour renseignements complémentaires, soit en raison de présentation matérielle erronée ou incomplète, soit le plus souvent en raison de l’insuffisance ou de l’imprécision des éléments ou des indices nécessaires pour caractériser les présomptions d’implication personnelle et directe de l’objectif ou la proportionnalité et la subsidiarité de la prestation sollicitée.

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 législatives ou jurisprudentielles ou une atteinte aux droits et libertés. La Commission a adressé deux recommandations en 2010 :

- une recommandation a été adressée le 10 mai à M. le ministre de l’Intérieur pour rappeler aux services demandeurs selon la jurisprudence de la commission la seule obédience ou appartenance à une mouvance, fût-elle radicale ne suffit pas à étayer les présomptions d’une implication en lien avec des menées terroristes,
- une recommandation a été adressée le 31 août à la « personnalité qualifiée » sur la valeur de la description du comportement d’un objectif et les limites de cet indice en matière de présomption d’implication.

La CNCIS exerce un contrôle a posteriori sur la motivation des demandes validées par la « personnalité qualifiée », qui peut être défini comme gradué en ce qu’il s’agit :

- d’un contrôle modulé de l’exigence d’implication et de précision de la menace en fonction du caractère plus ou moins intrusif de la prestation sollicitée au regard des libertés individuelles ;

– d’emploi d’outils gradués en fonction des anomalies constatées. Ainsi la Commission recourt à la recommandation et à l’avertissement pour les demandes qui ne respectent pas les principes essentiels de la loi et de la jurisprudence. Pour les demandes dont l’analyse est plus complexe, la Commission met en œuvre un droit de suite permettant d’apprécier la pertinence de la mesure sollicitée. En 2010, pour une vingtaine de dossiers, la Commission a sollicité, via la « personnalité qualifiée », ce « droit de suite » afin que le service demandeur précise les résultats opérationnels, préventifs ou judiciaires de l’exploitation des données techniques de communications. 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.

– à titre préventif et par souci de prévisibilité, la Commission adresse des recommandations générales à la personnalité qualifiée et aux services soit par le biais de notes – cadre sur certains sujets en lien avec l’actualité des demandes ou à l’occasion des réunions mensuelles avec la personnalité qualifiée et ses adjoints. Ainsi 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 fait l’objet d’éclaircissements à plusieurs reprises au cours de l’année 2010. La qualification de certains actes ou de certains mouvements a fait l’objet de travaux conjoints avec les services et la personnalité qualifiée aux fins de veiller rigoureusement au respect du champ d’application de la loi du 23 janvier 2006 et à la définition légale pénale interne et internationale des infractions en lien avec des menées terroristes.

Deuxième partie

JURISPRUDENCE DE LA COMMISSION

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 de construction et de renouvellement d'interceptions de sécurité. En outre et comme cela a déjà été indiqué dans les éléments chiffrés relatant son activité, elle statue quotidiennement sur des demandes présentées sous la forme de l'urgence absolue.

La Commission exerce le contrôle de légalité sur ces demandes en mettant en œuvre deux principes, celui de la **proportionnalité** qui permet de mesurer l'implication de la cible et celui de la **subsidiarité** qui permet de s'assurer de l'absolue nécessité de recourir matériellement à l'interception.

Pour ce qui concerne l'examen de proportionnalité, la Commission réalise le travail initial de tout juriste pénaliste, c'est-à-dire la qualification des faits de leur articulation juridique avec le motif légal invoqué. C'est bien la qualité de la **motivation** des demandes qui va mécaniquement induire la possibilité puis la qualité de ce contrôle. Cette motivation doit donc être suffisante et pertinente.

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 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.

* * *

On détaillera 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 ingérence d'une autorité publique dans l'exercice de ce droit (droit au respect de la vie privée et familiale) que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

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

Les intérêts fondamentaux de la Nation sont 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 culturel. »

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

Rapidement (rapport 1994, p. 17 *sqq.*), la CNCIS a estimé que la notion de sécurité nationale devait bien être comprise au vu des dispositions du Nouveau Code pénal qui fait figurer cette notion parmi les intérêts fondamentaux de la Nation (article 410-1 du Code pénal) au même titre que l'intégrité du territoire, la forme républicaine des institutions ou les moyens de la défense.

S'il s'agit là d'un élargissement notable de la notion antérieure de sûreté de l'État, on ne saurait y voir pour autant une extension par assimilation aux atteintes les plus courantes à la sécurité des personnes ou des biens.

« La Commission a ainsi estimé utile de rappeler qu'il ne suffit pas d'invoquer la crainte générale d'un trouble à l'ordre public, comme y expose plus ou moins toute manifestation, pour répondre aux exigences de motivation résultant de la loi. Pour ce faire, il doit être justifié, avec la

précision nécessaire, d’une menace particulièrement grave à la sécurité nationale au sens ci-dessus rappelé ».

On relève dans le même rapport que :

- « la crainte d’un trouble à l’ordre public n’autorise le recours à une interception qu’en cas de menace particulièrement grave à la sécurité » ;
- « les interceptions de sécurité ne sauraient être utilisées comme moyen de pénétrer un milieu syndical ou politique ou de pratiquer la surveillance d’opposants étrangers, si la sécurité de l’État français lui-même n’est pas en cause. »

La Commission est restée fidèle à cette doctrine.

• S’agissant des troubles à l’ordre public, des demandes motivées par cette crainte peuvent parfois être présentées sans que soit cependant allégué le risque d’attenter à la forme républicaine des institutions ou de déboucher sur un mouvement insurrectionnel. Si des manifestations sont susceptibles de dégénérer, le droit de manifester étant constitutionnellement reconnu, il s’agit là, en principe, d’un problème d’ordre public et non d’une atteinte à la sécurité nationale. On peut cependant admettre que dans certaines hypothèses, l’ampleur des troubles ou la charge institutionnelle voulue par leurs auteurs affectant le lieu et le temps des manifestations, la qualité des autorités ou des symboles républicains visés, sont tels que la sécurité nationale peut être menacée.

• S’agissant de la recherche de renseignements, la personne dont on se propose d’intercepter les correspondances doit être suspectée d’attenter par ses agissements personnels aux intérêts fondamentaux de la Nation. Si les services de renseignements ont, par nature, une mission de collecte de renseignements qu’ils remplissent en utilisant la palette des moyens disponibles, le recours aux interceptions de sécurité connaît certaines limites. En effet, l’atteinte exceptionnelle à la vie privée qu’autorise la loi ne peut être justifiée même dans ce domaine que par la menace directe ou indirecte, actuelle ou future que la personne écouteée 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 motifs¹, 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 économiques³ ».

« 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 pays⁴ ».

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

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

2) *Cf. supra*.

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

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

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 ou organisations étrangères.

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

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

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

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

Il résulte de ce qui précède qu’en dépit de la définition extensive donnée au concept d’intelligence économique, les interceptions sollicitées sous le motif « sauvegarde des éléments essentiels du potentiel scientifique et économique de la France » dont la formulation est directement reprise du Code pénal renvoient 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.

Ces critères : 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 (infractions prévues par les articles 411-1 à 411-11 du Code pénal) vérifiable traduisant une intention de nuire aux intérêts d'une entreprise¹ 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 nationale² 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 n° 2009-1122 du 17 septembre relatif au Délégué interministériel à l'intelligence économique en constitue une illustration.

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 ».

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.

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**.

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

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

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

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

Sous l'empire de l'ancien Code pénal, était réputée «bande organisée tout groupement de malfaiteurs établi en vue de commettre un ou plusieurs vols aggravés [...] et caractérisé par une préparation ainsi que par la possession des moyens matériels utiles à l'action». C'était là une définition très restrictive quant à son champ d'application, réduite 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 prémeditation. 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 défini 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. Pénalemen, 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 cinq 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 prémeditation 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 1^{er} de la loi n° 91-646 du 10 juillet 1991 :

« Le secret des correspondances émises par la voie des “communications électroniques” est garanti par la loi. Il ne peut être porté atteinte à ce secret que par l'autorité publique dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci. »

Les interceptions légales de correspondances émises par la voie des «communications électroniques» sont de deux types, judiciaires et de sécurité. S'agissant des interceptions judiciaires, le pluriel est employé à dessein depuis l'entrée en vigueur des lois n° 2002-1138 du 9 septembre 2002 et 2004-204 du 9 mars 2004.

En effet, aux interceptions en matière criminelle et correctionnelle prévues par les articles 100 à 100-7 du Code de procédure pénale, s'ajoutent celles prévues par les dispositions suivantes du même Code :

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

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

Tableau récapitulatif des durées d'interceptions et conditions de renouvellement

	Autorité	Motif	Durée	Renouvellement
Interceptions de sécurité	Premier ministre (article 3, loi du 10 juillet 1991)	– 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	1 mois (la loi n° 2011-267 du 14 mars 2011)	Renouvelable 1 fois
Autres	Administration pénitentiaire sous le contrôle du procureur de la République* (article 727-1 CPP)	Prévention des évasions Sécurité et bon ordre des établissements pénitentiaires ou des établissements de santé habilités à recevoir des détenus	Temps de la détention <i>NB : 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</i>	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 téléphoniques peuvent être écoutées, enregistrées et interrompues.

Pour des raisons de clarté de présentation les dispositions relatives à ces interceptions seront présentées à la suite de celles des articles 100 à 107 du Code de procédure pénale auxquels elles renvoient même si elles ne font pas strictement partie du titre I^{er} de la loi de 1991.

Loi n° 91-646 du 10 juillet 1991 consolidée

Titre I (de la loi n° 91-646 du 10 juillet 1991 consolidée) :

DES INTERCEPTIONS ORDONNÉES PAR L'AUTORITÉ JUDICIAIRE

Les interceptions ordonnées en matière criminelle et correctionnelle

Code de procédure pénale

Livre I^{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 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 daucun 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 – Modifié par la loi n° 2010-1 du 4/1/2010 « 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 transcrives en français avec l’assistance d’un interprète requis à cette fin. »

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

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

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

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

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

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

Aucune interception ne peut avoir lieu sur une ligne dépendant du cabinet d’un magistrat ou de son domicile sans que le premier président ou le procureur général de la juridiction où il réside en soit informé. « Les formalités prévues par le présent article sont prescrites à peine de nullité. »

Les interceptions ordonnées pour recherche d’une personne en fuite

Code de procédure pénale

Livre I^{er} : De l’exercice de l’action publique et de l’instruction

Titre II : Des enquêtes de contrôle d’identité

Chapitre I^{er} : 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.

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 I^{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 de 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 – Modifié par la loi n° 2011-267 du 14 mars 2011 « Si les nécessités de l’enquête de flagrance ou de l’enquête préliminaire relative à l’une des infractions entrant dans le champ d’application de l’article 706-73 l’exigent, le juge des libertés et de la détention du tribunal de grande instance peut, à la requête du procureur de la République, autoriser l’interception, l’enregistrement et la transcription de correspondances émises par la voie des télécommunications selon les modalités prévues par les articles 100 deuxième alinéa, 100-1 et 100-3 à 100-7, pour une durée maximum d’un mois, 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 – Crée par la loi n° 2007-297 du 5 mars 2007 – article 72
JORF 7 mars 2007

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

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

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

Titre II (de la loi n° 91-646 du 10 juillet 1991 consolidée) :

DES INTERCEPTIONS DE SÉCURITÉ

Article 3 – «Peuvent être autorisées, à titre exceptionnel, dans les conditions prévues par l'article 4, les interceptions de correspondances émises par la voie des "communications électroniques" (loi 2004-669 du 9 juillet 2004) ayant pour objet de rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées.»

Article 4 – modifié par l'article 6 II de la loi n° 2006-64 du 23 janvier 2006 –

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

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

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

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

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

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

Cette transcription est effectuée par les personnels habilités. »

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

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

Il est dressé procès-verbal de cette opération. »

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

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

Article 11-1 – (*introduit par l’article 31 de la loi 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne*) – « Les personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité sont tenues de remettre aux agents autorisés dans les conditions prévues à l’article 4, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu’elles ont fournies. Les agents autorisés peuvent demander aux fournisseurs de prestations susmentionnés de mettre eux-mêmes en œuvre ces conventions, sauf si ceux-ci démontrent qu’ils ne sont pas en mesure de satisfaire à ces réquisitions.

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

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

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

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

Les opérations mentionnées aux alinéas précédents sont effec-
tuées 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 admi-
nistrative indépendante. Elle est chargée de veiller au respect des dis-
positions du présent titre. Elle est présidée par une personnalité dési-
gnée, 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'empêche-
ment 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 déro-
gation au septième alinéa ci-dessus, ils peuvent être nommés comme membre de la Commission s'ils ont occupé ces fonctions de remplace-
ment 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 connais-
sance en raison de leurs fonctions. La Commission établit son règlement intérieur. »

Article 14 – « La décision motivée du Premier ministre mentionnée à l'article 4 est communiquée dans un délai de quarante-huit heures au

plus tard au président de la Commission nationale de contrôle des interceptions de sécurité.

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

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

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

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

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

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

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

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

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

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

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

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

Article 19 – modifié par l'article 6 de la loi n° 2006-64 du 23 janvier 2006 – « La Commission remet chaque année au Premier ministre un rapport sur les conditions d'exercice et les résultats de son activité, qui précise notamment le nombre de recommandations qu'elle a adressées au Premier ministre en application de l'article 14 de la présente loi et au ministre de l'Intérieur en application de l'article L. 34-1-1 du Code des postes et des communications électroniques et de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, ainsi que les suites qui leur ont été données. Ce rapport est rendu public.

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

Titre III (de la loi n° 91-646 du 10 juillet 1991 consolidée) :

DISPOSITIONS COMMUNES AUX INTERCEPTIONS JUDICIAIRES ET DE SÉCURITÉ

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

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

Article 22 – (modifié par l'article 18 de la loi n° 96-659 du 26 juillet 1996 sur la réglementation des télécommunications) – « Les juridictions compétentes pour ordonner des interceptions en application du Code de procédure pénale ainsi que le Premier ministre ou, en ce qui concerne l'exécution des mesures prévues à l'article 20, le ministre de la Défense ou le ministre de l'Intérieur, peuvent recueillir, auprès des personnes physiques ou morales exploitant des réseaux de "communications électroniques" ou fournisseurs de services de "communications électroniques", les informations ou documents qui leur sont nécessaires, chacun en ce qui le concerne, pour la réalisation et l'exploitation des interceptions autorisées par la loi.

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

Le fait, en violation du premier alinéa, de refuser de communiquer les informations ou documents, ou de communiquer des renseignements

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

Article 23 – « Les exigences essentielles définies au 12^e 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 226-13¹ du Code pénal toute personne qui, concourant dans les cas prévus par la loi à l'exécution d'une décision d'interception de sécurité, révélera l'existence de l'interception. »

Titre IV (de la loi n° 91-646 du 10 juillet 1991 consolidée) :

COMMUNICATION DES DONNÉES TECHNIQUES RELATIVES À DES COMMUNICATIONS ÉLECTRONIQUES

Article 27 – « La Commission nationale de contrôle des interceptions de sécurité exerce les attributions définies à l'article L. 34-1-1 du Code des postes et des communications électroniques et à l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique en ce qui concerne les demandes de communication de données formulées auprès des opérateurs de communications électroniques et personnes mentionnées à l'article L. 34-1 du Code précité ainsi que des prestataires mentionnés aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 précitée. »

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

DISPOSITIONS FINALES

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

Textes réglementaires récents visant la loi du 10 juillet 1991

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

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

Article 1^{er} – « 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) Substitué dans le Nouveau Code pénal à l'article 378, mentionné dans la loi du 10 juillet 1991.

1) de soumettre au Premier ministre les propositions d’interception présentées dans les conditions fixées par l’article 4 de la loi du 10 juillet 1991 susvisée;

2) d’assurer la centralisation de l’exécution des interceptions de sécurité autorisées;

3) de veiller à l’établissement du relevé d’opération prévu par l’article 8 de la loi du 10 juillet 1991 susvisée, ainsi qu’à la destruction des enregistrements effectués, dans les conditions fixées par l’article 9 de la même loi. »

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

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

Décret n° 2002-997 du 16 juillet 2002 relatif à l’obligation mise à la charge des fournisseurs de prestations de cryptologie en application de l’article 11-1 de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des « communications électroniques » (JO du 18 juillet 2002)

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

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

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

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

Article 4 – « La décision mentionnée au premier alinéa de l’article 1^{er} :

a) indique la qualité des agents habilités à demander au fournisseur de prestations de cryptologie la mise en œuvre ou la remise des conventions, ainsi que les modalités selon lesquelles les données à déchiffrer lui sont, le cas échéant, transmises;

b) fixe le délai dans lequel les opérations doivent être réalisées, les modalités selon lesquelles, dès leur achèvement, le fournisseur remet

aux agents visés au a) du présent article les résultats obtenus ainsi que les pièces qui lui ont été éventuellement transmises;

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

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

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

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

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

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

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

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

Article 6

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

Article L. 34-1-1 – « Afin de prévenir [Dispositions déclarées non conformes à la Constitution par la décision du Conseil constitutionnel n° 2005-532 DC du 19 janvier 2006] les actes de terrorisme, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions

peuvent exiger des opérateurs et personnes mentionnés au I de l’article L. 34-1 la communication des données conservées et traitées par ces derniers en application dudit article.

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

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

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

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

II. – Après le II de l’article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique, il est inséré un II bis ainsi rédigé :

II bis – «Afin de prévenir [Dispositions déclarées non conformes à la Constitution par la décision du Conseil constitutionnel n° 2005-532 DC du 19 janvier 2006] les actes de terrorisme, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie

nationales spécialement chargés de ces missions peuvent exiger des prestataires mentionnés aux 1 et 2 du I la communication des données conservées et traitées par ces derniers en application du présent article.

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

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

III. – 1. À la fin de la seconde phrase du premier alinéa de l'article 4 de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, les mots : « ou de la personne que chacun d'eux aura spécialement déléguée » sont remplacés par les mots : « ou de l'une des deux personnes que chacun d'eux aura spécialement déléguées ». »

– **2.** Dans la première phrase du premier alinéa de l'article 19 de la même loi, les mots : « de l'article 14 et » sont remplacés par les mots : « de l'article 14 de la présente loi et au ministre de l'Intérieur en application de l'article L. 34-1-1 du Code des postes et des communications électroniques et de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, ainsi que ».

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

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

Titre IV (de la loi n° 91-646 du 10 juillet 1991 consolidée) :

**COMMUNICATION DES DONNÉES TECHNIQUES RELATIVES
À DES COMMUNICATIONS ÉLECTRONIQUES**

Article 27 – « La Commission nationale de contrôle des interceptions de sécurité exerce les attributions définies à l'article L. 34-1-1 du Code des postes et des communications électroniques et à l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique en ce qui concerne les demandes de communication de données formulées auprès des opérateurs de communications électroniques et personnes mentionnées à l'article L. 34-1 du code précité ainsi que des prestataires mentionnés aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 précitée. »

Cet article appelle les commentaires suivants :

- Sur la « personnalité qualifiée » :

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

- Sur le champ d’application de cet article :

Le Conseil constitutionnel a censuré au nom du principe de séparation des pouvoirs la disposition liminaire de l’article 6 consistant non seulement à prévenir mais également à réprimer le terrorisme (décision n° 2002-532 DC du 19 janvier 2006). Une séparation nette entre réquisitions judiciaires (*cf.* notamment article 77-1-1 du Code de procédure pénale) et réquisitions administratives (articles 22 de la loi du 10 juillet 1991 et 6 de la loi n° 2006-64 du 23 janvier 2006) est ainsi assurée identique à la séparation entre interceptions judiciaires (article 100 à 100-7 du Code de procédure pénale) et interceptions administratives à laquelle la CNCIS a toujours attaché du prix (3^e rapport 1994, p. 19; 7^e rapport 1998, p. 23; 8^e rapport 1999, p. 14).

Loi n° 2008-1245 du 1^{er} 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.

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

Troisième mission : le contrôle du matériel

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

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

- article 226-1 du Code pénal : réprimant les atteintes à la vie privée;
- article 226-15 du Code pénal : réprimant le détournement de correspondance.

Ce texte inclut, dans cette notion de détournement, le fait, de mauvaise foi : « d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions » ;

- article 226-3 du Code pénal : réprimant la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente, en l'absence d'autorisation ministérielle dont les conditions sont fixées par décret en Conseil d'État, d'appareils conçus pour réaliser les opérations pouvant constituer l'infraction prévue par l'article 226-15 du Code pénal.

• **Le décret 97-757 du 10 juillet 1997** qui met en œuvre, à la faveur des articles R. 226-1 à R. 226-12 du Code pénal, la procédure d'« autorisation ministérielle » prévue par l'article 226-3 du Code pénal. L'organisation de la Commission consultative placée sous la présidence du 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).

Ces textes sont reproduits ci-après :

• **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^e 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 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 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 œuvre de manière spécifique le régime relatif au « registre » prévu par l’article R. 226-10 du Code pénal (registre retraçant la gestion des matériels soumis à autorisation). Cet arrêté a emporté l’abrogation de l’arrêté du 15 janvier 1998 qui constituait jusqu’alors le siège de cette matière ;
- l’instruction du 5 septembre 2006, véritable documentation pédagogique à l’attention des « usagers » de la réglementation relative au matériel. Elle constitue un guide pratique efficace offrant une présentation claire des modalités procédurales d’examen des demandes, ainsi que des règles de compétence de la Commission consultative dite « R. 226 ».

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 1^{er}

Instruction des demandes

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

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

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

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

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

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

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

- les capacités à capter, enregistrer ou transmettre, sans le consentement de leurs auteurs, des paroles prononcées à titre privé ou confidentiel;
- les moyens éventuels de cryptologie intégrés ou intégrables dans le matériel;
- les moyens et méthodes permettant de prévenir l'usage non autorisé du matériel;

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

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

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

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

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

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

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

- les moyens éventuels de cryptologie intégrés ou intégrables dans le matériel;
- les moyens et méthodes permettant de prévenir l’usage non autorisé du matériel;

3° Le nombre d’appareils pour la détention desquels l’autorisation est demandée;

4° L’utilisation prévue et son cadre d’emploi;

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

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

Remarques :

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

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

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

Article 2

Compétence de la Commission consultative

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

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

La Commission émet un avis sur :

1. Les demandes d’autorisation et de renouvellement de plein droit

Conformément aux termes du troisième alinéa de l’article R. 226-9, l’autorisation mentionnée à l’article R. 226-7 du Code pénal (acquisition ou détention) de tout appareil figurant en annexe de l’arrêté du 29 juillet

2004 est accordée de plein droit aux agents ou services de l'État habilités à réaliser des interceptions autorisées par la loi, après avis de la Commission consultative réunie dans son format restreint.

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

2. Les demandes d'autorisation et de renouvellement

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

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

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

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

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

2 bis. L'exposition

L'exposition des matériels soumis à autorisation est exclusivement limitée auprès des personnes, services de l'État ou entreprises titulaires d'une autorisation d'acquisition ou de détention du matériel exposé. Elle ne permet pas la vente d'un matériel, sauf si l'autorisation signée par le secrétaire général de la défense nationale le précise.

3. Les contrôles

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

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

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

4. Des arrêtés

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

Article 3

Conditions d’octroi des avis techniques et de moralité

1. Les conditions d’octroi de l’avis technique

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

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

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

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

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

2. Les conditions d’octroi des avis de moralité

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

A – Du ministère de la Justice : son représentant fait connaître, lors de la réunion de la Commission consultative, les éventuelles observations qu’appellent les différentes demandes d’autorisation présentées ;

B – De la Direction générale des douanes : la Direction nationale du renseignement et des enquêtes douanières fait connaître au SGDN, lors de la réunion de la Commission consultative, les éventuelles observations qu’appellent les différentes demandes d’autorisation présentées ;

C – Du ministère de l'Intérieur : après enquête, la DGPN adresse au SGDN un avis sans objection ou un avis défavorable motivé dans le délai d'un mois;

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

3. Avis des membres de la Commission consultative

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

Article 4

Retraits d'autorisation

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

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

On peut classer ces retraits en deux catégories.

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

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

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

Ainsi, constitue un motif de retrait :

- s'agissant de l'ensemble des titulaires d'autorisation :
- le refus de se soumettre aux contrôles nécessaires à la vérification du respect des indications fournies dans la demande d'autorisation (articles R. 226-4 et R. 226-8);
- le non-respect des obligations dont est assortie l'autorisation (articles R. 226-5 et R. 226-9);
- s'agissant des titulaires d'une autorisation de fabrication, d'importation, d'exposition, d'offre, de location ou de vente :

- le fait de ne pas tenir un registre ou de refuser de le présenter aux services enquêteurs (article R. 226-10);
- le fait de ne pas avoir porté, sur chaque appareil fabriqué, importé, exposé, offert, loué ou vendu, la référence du type correspondant à la demande d’autorisation (article R. 226-6);
- le fait d’avoir proposé, cédé, loué ou vendu des appareils à des personnes ou sociétés non autorisées (article R. 226-10);
- le fait de réaliser une publicité en faveur d’un appareil susceptible de permettre la réalisation des infractions prévues par l’article R. 226-1 et le second alinéa de l’article 226-15 du Code pénal lorsque cette publicité constitue une incitation à commettre ces infractions.

B. – Le retrait de l’autorisation lié à une condamnation pénale :

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

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

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

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

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

Chapitre II

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.

Aux termes 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 résulte que la classification s’impose à tous les éléments relatifs à une interception de sécurité. Les interceptions de sécurité intéressent la défense nationale et les informations qui y sont relatives sont revêtues de la mention secret-défense.

Cette classification fonde la restriction de l’information du requérant à la notification de l’accomplissement du contrôle de légalité et du respect des dispositions légales.

Cette position, adoptée dès ses débuts par la CNCIS, correspond à la volonté exprimée par le législateur devant les travaux parlementaires d’une application stricte de l’article 17 de la loi du 10 juillet 1991.

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). La Commission ne précise pas si une interception de sécurité a été effectivement mise en œuvre ou pas.

Cette position est fondée sur le respect des dispositions législatives relatives au secret de la défense nationale, notamment celles relatives à la compromission de ce secret.

Ces dispositions ont été abondées au cours de l’année 2010 par la publication de plusieurs textes réglementaires pris en application de la loi de programmation militaire du 29 juillet 2009 sur la protection du secret de la défense. Il s’agit :

- du décret n° 2010-678 du 23 juin 2010 relatif à la protection du secret de la défense nationale,
- de l'arrêté du 21 juin 2010 fixant en application de l'article R2311-9-1 du code la défense la liste des lieux abritant des éléments couverts par le secret de la défense nationale,
- de l'arrêté du 21 juin 2010 portant en application de l'article R2311-9-3 du code de la défense, décision de classification de lieux
- de l'arrêté du 23 juillet 2010 portant approbation de l'instruction générale interministérielle sur la protection du secret de la défense nationale

Ces textes visent à renforcer la sécurité juridique de la protection du secret de la défense en tenant compte de l'effacement du clivage traditionnel entre défense et sécurité. Ils rappellent que la protection du secret concerne tous les domaines d'activité relevant de la défense et de la sécurité nationale, politique, militaire, diplomatique, scientifique, économique, industriel.

Ces textes reprennent pour leur mise en œuvre les nouvelles dispositions sur les lieux protégés par le secret de la défense nationale précisant les conditions dans lesquels les magistrats peuvent désormais pénétrer dans ces lieux protégés et y saisir les objets classifiés (documents, rapports, CD ROM, comptes rendus et transcriptions d'écoutes...) en étant accompagnés du président de la commission consultative du secret de la défense nationale, gardien des objets classifiés mis sous scellés dans l'attente de leur examen par la dite commission, qui émet alors un avis au ministre concerné, au premier ministre ou au président de la république c'est-à-dire, l'autorité à l'origine de la classification de ces documents.

Chapitre III

Éléments de jurisprudence et actualités parlementaires

Jurisprudence européenne

Communiqué du Greffier

Arrêt de chambre
Non définitif¹

Kennedy c. Royaume-Uni (requête n° 26839/05)

DES MESURES DE SURVEILLANCE SECRÈTE N'ONT PAS PORTÉ ATTEINTE À LA VIE PRIVÉE DU REQUÉRANT

A l'unanimité :

Non-violation de l'article 8 (droit au respect de la vie privée et familiale et de la correspondance)

Non-violation de l'article 6 § 1 (droit à un procès équitable)

*Non-violation de l'article 13 (droit à un recours effectif)
de la Convention européenne des droits de l'homme*

Principaux faits

Le requérant, Malcolm Kennedy, est un ressortissant britannique né en 1946 et résidant à Londres. Arrêté pour ivresse en 1990, il passa la nuit en détention avec un autre détenu, lequel fut trouvé mort le lendemain. Le requérant fut déclaré coupable d'homicide et condamné à la prison à perpétuité. Cette affaire suscita une polémique au Royaume-Uni, eu égard au manque de preuves et à l'existence d'éléments contradictoires.

Remis en liberté en 1996, M. Kennedy monta une entreprise de déménagement. Par la suite, il affirma que son courrier professionnel, ses conversations téléphoniques et ses courriels étaient interceptés parce que sa cause avait été médiatisée et qu'il avait par la suite milité contre les erreurs judiciaires.

Le requérant se plaignit auprès de la Commission des pouvoirs d'enquête (CPE) que ses communications étaient interceptées dans des « circonstances contestables » s'analysant en une violation de sa vie privée. Il tenta d'obtenir l'interdiction de toute interception de ses communications par les services de renseignement et la « destruction de tout produit issu d'une telle interception ». Il demanda également des instructions spécifiques afin que soit garantie l'équité de la procédure devant la CPE, notamment une audience publique et un contrôle réciproque, entre les parties, des témoignages et éléments de preuve.

La CPE examina à huis clos les griefs spécifiques du requérant et, en 2005, jugea qu'aucune décision favorable n'était rendue quant à ses plaintes, ce qui signifiait soit qu'il n'y avait pas eu interception de communications, soit que toute interception ayant eu lieu avait été légale.

1) 18 mai 2010.

Griefs, procédure et composition de la Cour

Invoquant l’article 8, le requérant se plaignait de l’interception alléguée de ses communications. Sur le terrain de l’article 6 § 1, il affirmait par ailleurs que l’audience devant la CPE avait été inéquitable et, sous l’angle de l’article 13, qu’il avait dès lors été privé d’un recours effectif.

La requête a été introduite devant la Cour européenne des droits de l’homme le 12 juillet 2005.

L’arrêt a été rendu par une chambre de sept juges composée de :

Lech Garlicki (Pologne), *président*,
Nicolas Bratza (Royaume-Uni),
Giovanni Bonello (Malte),
Ljiljana Mijović (Bosnie-Herzégovine),
Päivi Hirvelä (Finlande),
Ledi Bianku (Albanie),
Nebojša Vučinić (Monténégro), *Juges*,

ainsi que de Lawrence Early, *greffier de section*.

Décision de la Cour

Article 8

La Cour rappelle que, sur le fondement du principe de protection effective offerte par le mécanisme de la Convention, un individu peut – sous certaines conditions qui doivent être définies dans chaque affaire – se prétendre victime d’une violation entraînée par la simple existence de mesures secrètes, même si elles ne lui ont pas été appliquées. Cette dérogation à l’approche générale de la Cour vise à garantir que de telles mesures, bien que secrètes, puissent être contestées et contrôlées par une autorité judiciaire. En l’espèce, la Cour estime qu’il ne peut être exclu que des mesures de surveillance secrète aient été appliquées au requérant ou qu’il ait été, à l’époque des faits, susceptible d’en être l’objet. En conséquence, elle conclut que M. Kennedy est fondé à se plaindre d’une atteinte à ses droits découlant de l’article 8.

Pour la Cour, il est manifeste que l’ingérence en question poursuivait les buts légitimes qui consistent à protéger la sécurité nationale et le bien-être économique du pays ainsi qu’à prévenir les infractions pénales. Par ailleurs, cette ingérence reposait sur la loi de 2000 portant réglementation des pouvoirs d’enquête (« la RIPA »), complétée par le code de conduite en matière d’interception de communications (« le code »). La RIPA était accessible dès lors qu’elle était consultable sur internet. Elle définissait avec une précision suffisante les cas dans lesquels il pouvait y avoir interception de communications. Certes, les infractions justifiant une interception n’étaient pas nommées ; cependant, la Cour observe que les Etats ne sont pas tenus de dresser une liste exhaustive des atteintes à la sécurité nationale, celles-ci étant par essence difficiles à définir par avance. Enfin, seules les communications internes au Royaume-Uni ayant été concernées en l’espèce – ce qui n’était pas le cas dans l’affaire *Liberty et autres c. Royaume-Uni*² –, il y a lieu de signaler que le droit interne décrivait plus précisément les catégories de personnes pouvant être visées par une interception de communications.

En ce qui concerne le traitement, la communication et la destruction des données, la Cour relève que la durée globale des mesures d’interception doit être laissée à l’appréciation des autorités internes, tant que des garanties adéquates sont mises en place. En l’espèce, le renouvellement ou l’annulation des mandats d’interception faisaient l’objet d’un contrôle systématique du ministre. De plus, contrairement à la pratique concernant les communications avec d’autres pays, le droit national disposait que les mandats relatifs aux communications internes devaient porter uniquement sur une personne ou sur un ensemble de lieux, ce qui limitait l’étendue du pouvoir discrétionnaire des autorités d’intercepter et d’écouter des communications privées. Par ailleurs, le droit – plus

précisément le code – limitait strictement le nombre de personnes ayant accès au matériel intercepté, dont seul un résumé était divulgué si cela suffisait. En outre, le droit interne exigeait la destruction des données dès que celles-ci n'étaient plus nécessaires, ainsi que la conservation d'informations détaillées sur les mandats.

Du point de vue du contrôle du régime RIPA, la législation prévoit la désignation d'un commissaire, qui est indépendant des pouvoirs exécutif et législatif. Son rapport annuel à l'intention du premier ministre est un document public qui est présenté au Parlement. La Cour juge très précieux le rôle du commissaire consistant à s'assurer de la bonne application des dispositions légales, de même que son contrôle, deux fois par an, sur une sélection aléatoire d'affaires dans lesquelles une interception a été autorisée. Par ailleurs, la Cour souligne la large compétence de la CPE pour examiner toute plainte pour interception illégale de communications. Tout citoyen peut saisir la CPE – organe indépendant et impartial –, droit qui dans de nombreux autres pays n'a pas d'équivalent. La CPE a accès aux documents secrets et peut prier le commissaire d'ordonner la divulgation de tout document jugé pertinent par elle. Lorsqu'elle rend une décision favorable au demandeur, elle peut annuler un ordre d'interception, demander la destruction de matériel intercepté ou ordonner une réparation. La publication des décisions de la CPE ne fait que renforcer le niveau de contrôle sur les activités de surveillance secrète menées au Royaume-Uni.

La Cour conclut qu'en l'espèce les décisions pertinentes du droit interne présentaient avec une clarté suffisante les procédures concernant les mandats d'interception ainsi que le traitement, la communication et la destruction des données recueillies. La Cour observe enfin qu'aucun élément n'indique qu'il y ait eu d'importantes lacunes dans l'application et la mise en œuvre du régime de surveillance. Dès lors, il n'y a pas eu violation de l'article 8.

Article 6 § 1

La Cour rappelle que le droit à un procès pleinement contradictoire peut être restreint dans la mesure strictement nécessaire à la sauvegarde d'un intérêt public important. Les restrictions appliquées dans la procédure de la CPE étaient justifiées par des considérations de confidentialité, et la nature des questions soulevées légitimait l'absence d'une audience publique. Par ailleurs, la Cour note qu'en vertu de l'article 6 § 1 de la Convention, la sécurité nationale peut justifier que le public soit écarté d'une procédure. Quant à la politique des autorités consistant à « ne pas confirmer et ne pas démentir » – *décision de la CPE de 2005* – la Cour juge suffisant qu'un demandeur soit informé de cette manière.

Elle souligne qu'une personne souhaitant se plaindre d'une interception de communications au Royaume-Uni a largement et facilement accès à la CPE. Consciente de l'importance que revêt la surveillance secrète dans la lutte contre le terrorisme et les crimes graves, la Cour estime que les restrictions aux droits du requérant dans le cadre de la procédure devant la CPE étaient nécessaires et proportionnées, et non contraires à l'article 6.

Article 13

Compte tenu de ses conclusions sous l'angle des articles 8 et 6 § 1, la Cour considère que la CPE a offert au requérant un recours effectif pour autant que son grief concernait l'interception alléguée de ses communications. S'agissant de son grief général tiré de l'article 8, la Cour réaffirme que l'article 13 ne va pas jusqu'à exiger un recours par lequel on puisse dénoncer, devant une autorité nationale, les lois d'un État contractant comme contraires à la Convention ou à des normes de droit internes équivalentes. Dès lors, la Cour rejette le grief du requérant tiré de l'article 13.

620

02.09.2010

Communiqué du Greffier

Arrêt de chambre

Non définitif¹

Uzun c. Allemagne (requête n° 35623/05)

**LA SURVEILLANCE PAR GPS D'UNE PERSONNE SOUPÇONNÉE D'INFRACTIONS GRAVES
ETAIT JUSTIFIÉE**

A l'unanimité :

Non-violation de l'article 8 (droit au respect de la vie privée et familiale)

Non-violation de l'article 6 § 1 (droit à un procès équitable)

de la Convention européenne des droits de l'homme

Principaux faits

Le requérant, Bernhard Uzun, est un ressortissant allemand né en 1967 et résidant à Mönchengladbach (Allemagne). L'affaire concerne la surveillance de l'intéressé par GPS (système de géolocalisation par satellite) dans le cadre d'une enquête pénale. C'est la première affaire concernant une telle surveillance dont la Cour européenne des droits de l'homme ait été saisie.

En octobre 1995, le procureur général près la Cour fédérale de Justice (*Generalbundesanwalt*) ouvrit une instruction contre M. Uzun et un complice présumé pour participation à des attentats à la bombe revendiqués par la « cellule anti-impérialiste », une organisation qui poursuivait la lutte armée abandonnée en 1992 par la Fraction armée rouge (RAF), mouvement terroriste d'extrême gauche.

L'Office fédéral de la police judiciaire (*Bundeskriminalamt*) fut chargé de l'enquête. Il procéda notamment à la surveillance visuelle de M. Uzun pendant les week-ends, à la surveillance au moyen d'une caméra vidéo de l'entrée de l'immeuble où l'intéressé vivait, à des écoutes téléphoniques et à l'installation d'émetteurs dans la voiture du complice présumé, que celui-ci et le requérant utilisaient souvent ensemble. Les intéressés ayant découvert les dispositifs et les ayant détruits et étant donné qu'ils évitèrent de se parler au téléphone, le procureur général ordonna leur surveillance par GPS. L'Office fédéral de la police judiciaire installa un récepteur GPS dans le véhicule du complice présumé de M. Uzun en décembre 1995, ce qui lui permit de localiser la voiture. Cette surveillance dura jusqu'à l'arrestation des deux hommes, en février 1996.

Dans le cadre de la procédure pénale ouverte contre les deux hommes, la cour d'appel de Düsseldorf rejeta l'objection de M. Uzun à l'utilisation en tant que preuves des informations obtenues grâce à la surveillance par GPS. Elle estima que le recours au GPS était autorisé par le code de procédure pénale et qu'aucune décision judiciaire n'était nécessaire à cette fin. En septembre 1999, la cour d'appel condamna le requérant à une peine de treize ans d'emprisonnement pour tentative de meurtre et pour quatre attentats à la bombe. Elle conclut que les deux hommes avaient posé des bombes devant le domicile de députés et d'anciens députés et devant un consulat. Les éléments de preuve comprenaient les données obtenues grâce à la surveillance par GPS, lesquelles étaient corroborées par les renseignements recueillis au moyen d'autres méthodes de surveillance. M. Uzun se pourvut en cassation, se plaignant en particulier de l'utilisation au procès d'éléments de preuve obtenus grâce à sa surveillance par GPS. En janvier 2001, la Cour fédérale de Justice

1) 2 septembre 2010.

(*Bundesgerichtshof*) le débouta.

En avril 2005, la Cour constitutionnelle fédérale (*Bundesverfassungsgericht*) écarta le recours de M. Uzun. Elle estima que l'atteinte causée au droit de l'intéressé au respect de sa vie privée par sa surveillance par GPS était proportionnée, eu égard à la gravité des infractions et au fait qu'il s'était dérobé à d'autres mesures de surveillance. Pour la Cour constitutionnelle fédérale, les garanties procédurales en place étaient suffisantes pour éviter une surveillance totale permettant de dresser le profil exhaustif d'une personne. Toutefois, le législateur devait examiner si, eu égard à l'évolution future, ces garanties étaient suffisantes pour fournir une protection effective des droits fondamentaux et éviter la mise en œuvre non coordonnée de mesures d'enquête par différentes autorités.

Griefs, procédure et composition de la Cour

Le requérant alléguait que sa surveillance par GPS et l'utilisation des données ainsi obtenues dans le cadre de la procédure pénale dirigée contre lui avaient emporté violation de ses droits garantis par l'article 8. Ces données ayant constitué le fondement essentiel de sa condamnation, il se plaignait en outre d'une violation de l'article 6 § 1.

La requête a été introduite devant la Cour européenne des droits de l'homme le 24 septembre 2005.

L'arrêt a été rendu par une chambre de sept juges composée de :

Peer Lorenzen (Danemark), *président*,

Renate Jaeger (Allemagne),

Karel Jungwiert (République tchèque).

Mark Villiger (Liechtenstein),

Isabelle Berro-Lefèvre (Monaco),

Mirjana Lazarova Trajkovska (« l'ex-République yougoslave de Macédoine »)

Ganna Yudkivska (Ukraine), *Juges*,

et de Claudia Westerdiek, *greffière de section*.

Décision de la Cour

La Cour observe tout d'abord que le récepteur GPS a été intégré sur une voiture appartenant à un tiers (le complice de M. Uzun). Toutefois, en procédant de la sorte, les autorités d'enquête avaient manifestement l'intention de recueillir des informations sur les déplacements des deux suspects, étant donné que leurs précédentes investigations leur avaient révélé que ceux-ci avaient utilisé la voiture ensemble. On n'a pu faire le lien entre les déplacements de la voiture du complice et M. Uzun qu'en soumettant celui-ci à une surveillance visuelle supplémentaire et aucune des juridictions internes n'a contesté que l'intéressé avait été soumis à une surveillance par GPS.

Les autorités d'enquête ont systématiquement recueilli et conservé des données indiquant l'endroit où se trouvait M. Uzun et les déplacements de celui-ci en public. Elles ont de surcroît utilisé ces données pour suivre tous les déplacements de l'intéressé, pour effectuer des investigations complémentaires et pour recueillir d'autres éléments de preuve dans les endroits où il s'était rendu, éléments qui ont ensuite été utilisés dans le cadre du procès pénal.

La Cour estime que les aspects susmentionnés suffisent pour conclure que la surveillance de M. Uzun par GPS s'analyse en une ingérence dans l'exercice par lui de son droit au respect de sa vie privée garanti par l'article 8 § 1.

Sur le point de savoir si cette ingérence était « prévue par la loi », la Cour estime qu'elle avait une base dans le code de procédure pénale. Elle souligne qu'il y a lieu de distinguer la surveillance par GPS de déplacements en public d'autres méthodes de surveillance par des moyens visuels ou acoustiques car elle révèle moins d'informations sur la conduite, les opinions ou les sentiments de la personne qui en fait l'objet et porte donc moins atteinte au droit de celle-ci au respect de sa vie privée. La Cour ne voit donc pas la nécessité d'appliquer les mêmes garanties strictes contre les abus que celles qu'elle a développées dans sa jurisprudence sur la surveillance des télécommunications, par exemple l'obligation de définir précisément la durée maximale de l'exécution de la mesure de surveillance ou la procédure à suivre pour l'utilisation et la conservation des données recueillies.

La Cour estime que la conclusion unanime des juridictions internes selon laquelle la surveillance par GPS était couverte par le droit interne était raisonnablement prévisible, étant donné que les dispositions pertinentes prévoient le recours à des moyens techniques, en particulier « pour localiser l'auteur d'une infraction ». En outre, le droit interne subordonnait l'autorisation de la mesure de surveillance par GPS à des conditions très strictes ; en effet, une telle surveillance ne pouvait être ordonnée qu'à l'égard d'une personne soupçonnée d'une infraction extrêmement grave.

La Cour se félicite des modifications apportées au droit allemand après l'enquête menée dans l'affaire de M. Uzun car elles ont eu pour effet de renforcer la protection du droit d'un suspect au respect de sa vie privée, la surveillance systématique de celui-ci devant être ordonnée par un juge lorsqu'elle dépasse une durée d'un mois. Elle note toutefois que déjà en vertu des dispositions en vigueur à l'époque des faits la surveillance d'un individu par GPS était susceptible d'un contrôle judiciaire. Elle estime que le contrôle judiciaire ultérieur de la surveillance de M. Uzun par GPS a offert une protection suffisante contre l'arbitraire en l'espèce. Un tel contrôle, qui permet d'exclure les éléments de preuve obtenus au moyen d'une surveillance illégale par GPS, constitue une garantie importante, en ce qu'elle décourage les autorités d'enquête de recueillir des preuves par des moyens illégaux. La Cour conclut que l'ingérence dans l'exercice par M. Uzun de son droit au respect de sa vie privée était « prévue par la loi ».

La Cour note que la surveillance M. Uzun par GPS, ordonnée aux fins d'enquêter sur plusieurs accusations de tentatives de meurtre revendiquées par un mouvement terroriste et de prévenir d'autres attentats à la bombe, était dans l'intérêt de la sécurité nationale, de la sûreté publique, de la prévention des infractions pénales et de la protection des droits des victimes. La surveillance par GPS a seulement été ordonnée après que d'autres mesures d'investigation, moins attentatoires à la vie privée, se furent révélées moins efficaces, et cette mesure a été mise en œuvre pendant une période relativement courte (trois mois) et n'a touché l'intéressé que lorsqu'il se déplaçait dans la voiture de son complice. Dès lors, on ne saurait dire que le requérant a été soumis à une surveillance totale et exhaustive. L'enquête ayant porté sur des infractions très graves, la Cour estime que la surveillance de M. Uzun par GPS était proportionnée aux buts poursuivis.

La Cour conclut, à l'unanimité, à la non-violation de l'article 8 de la Convention. En outre, eu égard à cette conclusion, elle dit, à l'unanimité, qu'aucune question distincte ne se pose sous l'angle de l'article 6 § 1.

Communiqué du Greffier

Arrêt de chambre

Non définitif¹Dink c. Turquie (requêtes n°s 2668/07, 6102/08, 30079/08, 7072/09 et 7124/09)

À l'unanimité :

LES AUTORITÉS ONT MANQUÉ À LEUR DEVOIR DE PROTÉGER LA VIE ET LA LIBERTÉ D'EXPRESSION DU JOURNALISTE FIRAT (HRANT) DINK

*Deux violations de l'article 2 (droit à la vie ; absence d'enquête effective),
violation de l'article 10 (liberté d'expression) et
Violation de l'article 13 (droit à un recours effectif) combiné avec l'article 2
de la Convention européenne des droits de l'homme*

Principaux faits

Les requérants sont six ressortissants turcs : Firat Dink, connu sous le nom de plume Hrant Dink, son épouse (Rahil Dink), son frère (Hasrof Dink), et les trois enfants de Firat et Rahil Dink (Delal Dink, Arat Dink et Sera Dink). Firat Dink est né en 1954 et a été assassiné le 19 janvier 2007. Les autres requérants sont nés respectivement en 1959, 1957, 1978, 1979 et 1986 et résident à Istanbul. Journaliste turc d'origine arménienne, Firat Dink était directeur de publication et rédacteur en chef de l'hebdomadaire turco-arménien Agos, journal bilingue édité à Istanbul depuis 1996.

Entre novembre 2003 et février 2004, Firat Dink publia dans le journal Agos huit articles où il exposait son point de vue sur la question de l'identité des citoyens turcs d'origine arménienne. Il écrivait notamment, dans les sixième et septième articles de la série, que l'obsession de voir reconnaître leur qualité de victimes d'un génocide devenait la raison d'être des Arméniens, que ce besoin des Arméniens se heurtait à l'indifférence des Turcs et que cela expliquait que le traumatisme des Arméniens restait vivace. Selon lui, l'élément turc de l'identité arménienne était en même temps un poison et un antidote. Il ajoutait que l'identité arménienne pouvait se libérer de sa composante turque de deux façons : soit les Turcs montreraient de l'empathie pour les Arméniens – mais cela était difficilement réalisable à court terme –, soit les Arméniens se libéreraient de l'élément turc en élaborant une qualification autonome des événements de 1915 par rapport à celle retenue par le monde entier et par les Turcs. Dans son huitième article, Firat Dink, suivant la logique du reste de la série, écrivait « le sang propre qui se substituera à celui empoisonné par le « Turc » se trouve dans la noble veine reliant l'Arménien à l'Arménie, pourvu que l'Arménien en soit conscient ». M. Dink estimait que les autorités arméniennes devaient s'employer plus activement à renforcer les liens de la diaspora avec le pays, ce qui permettrait une construction plus saine de l'identité nationale. Il publia encore un article mentionnant l'origine arménienne de la fille adoptive d'Atatürk. Des groupes ultranationalistes réagirent à ces publications par des manifestations et lettres de menaces.

En février 2004, un militant ultranationaliste déposa une plainte pénale contre Firat Dink, soutenant qu'il avait insulté les Turcs par la phrase « le sang propre qui se substituera à celui empoisonné par le « Turc » se trouve dans la noble veine reliant l'Arménien à l'Arménie ». En avril 2004, le parquet de Şişli (Istanbul) intenta contre Firat Dink une action pénale en vertu de l'article du code pénal turc réprimant le dénigrement de « la turcité (Türklük) » (l'identité turque). En mai 2005, une expertise conclut que les propos de Firat Dink n'insultaient ni ne dénigraient personne, car ce qu'il qualifiait de « poison » n'était pas le sang turc, mais l'obsession des Arméniens à faire reconnaître que les

1) 14 septembre 2010.

événements de 1915 constituaient un génocide. En octobre 2005, le tribunal correctionnel de Şişli déclara Firat Dink coupable d'avoir dénigré la turcité et le condamna à six mois de prison avec sursis. Il estima que le lecteur ne devait pas avoir à lire toute la série d'articles pour comprendre le véritable sens de ses propos. Le 1^{er} mai 2006, la Cour de cassation (9^e chambre pénale) confirma le jugement quant au verdict de culpabilité. Le 6 juin 2006, le procureur général près la Cour de cassation forma un pourvoi extraordinaire, estimant que les propos de Firat Dink avaient été mal interprétés et que sa liberté d'expression devait être protégée. Le 11 juillet 2006, les chambres pénales réunies de la Cour de cassation rejetèrent ce pourvoi. Le 12 mars 2007, le tribunal correctionnel devant lequel le dossier avait été renvoyé déclara l'affaire close en raison du décès de Firat Dink.

Le 19 janvier 2007, à Istanbul, Firat Dink fut assassiné de trois balles dans la tête. L'auteur présumé de l'attentat fut arrêté à Samsun (Turquie). En avril 2007, le parquet d'Istanbul intenta une action pénale contre dix-huit accusés. Cette procédure est toujours en cours.

En février 2007, les inspecteurs du ministère de l'Intérieur et de la gendarmerie ouvrirent une enquête afin d'examiner si la gendarmerie de Trabzon avait commis une négligence ou une défaillance dans la prévention de l'assassinat, dans la mesure où un informateur soutenait avoir prévenu deux sous-officiers de la gendarmerie de ce crime. Les gendarmes nièrent avoir été mis au courant des préparatifs de l'assassinat. La préfecture de Trabzon autorisa l'ouverture d'une action pénale contre les deux sous-officiers, mais pas contre leurs supérieurs. Les sous-officiers reconnaissent finalement qu'un informateur les avait prévenus de l'éventualité de l'assassinat et précisèrent qu'ils en avaient à leur tour informé dans les moindres détails leurs supérieurs hiérarchiques, auxquels il incomba de prendre des mesures sur le fondement des renseignements recueillis. Ils déclarèrent également que c'était sur ordre de leurs supérieurs qu'ils avaient nié, lors de l'enquête, avoir reçu les renseignements en question. Cette procédure est toujours en cours.

Le parquet d'Istanbul saisit par ailleurs le parquet de Trabzon contre les responsables de la sûreté de Trabzon, au motif que l'un des accusés, par ailleurs informateur de la police de Trabzon, avait également fourni à la police des renseignements sur les préparatifs de l'assassinat. Les responsables de la police de Trabzon n'avaient rien tenté pour faire obstacle à ces projets mais s'étaient contentés d'informer officiellement les services de sûreté d'Istanbul de la probabilité de cet assassinat. Il ajouta que l'un des chefs de la police de Trabzon avait affiché ses opinions ultranationalistes et soutenu les accusés. Le 10 janvier 2008, le parquet de Trabzon rendit une ordonnance de non-lieu à l'égard des responsables de la sûreté de Trabzon. Il releva notamment que les accusations du parquet d'Istanbul reposaient sur la déposition de l'un des accusés, qui était revenu sur cette déposition. Il jugea convaincant l'argument selon lequel les policiers de Trabzon avaient estimé que les renseignements rassemblés n'étaient pas crédibles. Enfin, il souligna que le chef de la police soupçonné d'avoir soutenu les agissements des accusés niait les faits qui lui étaient reprochés. L'opposition des requérants à ce non-lieu fut rejetée.

L'enquête menée par le parquet d'Istanbul confirma que, le 17 février 2006, la sûreté de Trabzon avait officiellement informé la sûreté d'Istanbul de la probabilité de l'assassinat de Firat Dink, en précisant l'identité des personnes suspectes. La sûreté d'Istanbul n'aurait pas réagi à cette information. Suivant les conclusions de trois enquêtes menées à propos de cette inaction, le conseil d'administration de la préfecture d'Istanbul décida de traduire devant la justice pénale certains membres des services de sûreté d'Istanbul pour leur négligence. La cour administrative régionale d'appel d'Istanbul annula toutefois ces ordonnances du fait de l'insuffisance de l'enquête.

Enfin, sur plainte des requérants, une enquête pénale fut menée contre des membres de la sûreté et de la gendarmerie de Samsun pour apologie du crime. Pendant la garde à vue de l'auteur présumé de l'assassinat, ils s'étaient fait photographier en compagnie du suspect, qui portait dans les mains un drapeau turc ; en arrière-plan on pouvait lire au mur « la patrie est sacrée, son sort ne peut être laissé au hasard ». En juin 2007, le parquet de Samsun rendit un non-lieu à l'égard des agents mis en cause, jugeant que l'apologie d'un crime ne pouvait être faite que publiquement. Des sanctions disciplinaires furent néanmoins prises.

Griefs, procédure et composition de la Cour

Invoquant en particulier l'article 2, les requérants autres que Fırat Dink se plaignaient d'un manquement de l'Etat à son obligation de protéger la vie de Fırat Dink. Sur la base du même article, ils se plaignaient également de l'ineffectivité des poursuites pénales dirigées contre les agents publics pour n'avoir pas protégé la vie du journaliste. Sur ce point, ils invoquaient aussi l'article 13. Invoquant en particulier l'article 10, les requérants alléguait de surcroit que le fait de déclarer Fırat Dink coupable de dénigrement de la turcité a porté atteinte à sa liberté d'expression et a fait de lui une cible pour les ultranationalistes.

La requête a été introduite devant la Cour européenne des droits de l'homme le 11 janvier 2007 par le requérant Fırat Dink, et les autres requêtes ont été introduites respectivement le 18 décembre 2007, le 21 mai, le 27 novembre et le 22 décembre 2008 par Rahil, Delal, Arat et Sera Dink après le décès de Fırat Dink. Par ailleurs, dans la requête n° 7072/09, Hasrof Dink est aussi requérant.

L'arrêt a été rendu par une chambre de sept juges composée de :

Françoise Tulkens (Belgique), *présidente*,
Ireneu Cabral Barreto (Portugal),
Dragoljub Popović (Serbie),
András Sajó (Hongrie),
Nona Tsotsoria (Géorgie),
İşıl Karakaş (Turquie),
Guido Raimondi (Italie), *juges*,

ainsi que de Stan Naismith, *greffier de section*.

Décision de la Cour

Grief relatif au manquement allégué de l'Etat turc à protéger la vie de Fırat Dink (article 2)

La Cour estime que l'on peut raisonnablement considérer que les forces de l'ordre étaient informées de l'hostilité intense des milieux nationalisés contre Fırat Dink. Les enquêtes menées par le paquet d'Istanbul et les inspecteurs du ministère de l'Intérieur ont mis en évidence que tant la police de Trabzon et celle d'Istanbul que la gendarmerie de Trabzon avaient été informées de la probabilité de cet assassinat et même de l'identité des personnes soupçonnées d'en être les instigateurs. Vu les circonstances, ce risque d'assassinat pouvait passer pour réel et imminent.

La Cour examine ensuite la question de savoir si les autorités ont fait tout ce que l'on pouvait raisonnablement attendre d'elles pour empêcher que Fırat Dink soit assassiné. Or, aucune des trois autorités informées de la planification de l'assassinat et de son exécution imminente n'a réagi afin de l'empêcher. Certes, comme le Gouvernement turc l'a mis en avant, Fırat Dink n'a pas demandé de protection policière. Cependant, il était impossible pour lui d'avoir des renseignements sur le projet d'assassinat. C'est aux autorités turques, informées de ce projet, qu'il appartenait d'agir afin de protéger la vie de Fırat Dink.

Il y a donc eu violation de l'article 2 (sous son « volet matériel »)

Grief relatif à l'ineffectivité alléguée des enquêtes pénales (article 2)

La Cour examine les procédures pénales ouvertes après l'enquête, minutieuse et détaillée, menée concernant la manière dont les forces de l'ordre de Trabzon et Istanbul ont géré les informations obtenues sur le projet d'assassinat.

Elle note tout d'abord que la préfecture a refusé d'autoriser de traduire devant la justice pénale les officiers de la gendarmerie de Trabzon, à l'exception de deux sous-officiers. Aucune décision de

justice n'a été rendue sur le point de savoir pourquoi les officiers, compétents pour prendre les mesures appropriées suite à la transmission des renseignements par les sous-officiers, sont restés inactifs. En outre, les sous-officiers ont dû faire de fausses déclarations aux inspecteurs. Il s'agit là d'un manquement manifeste au devoir de prendre des mesures en vue de recueillir des preuves concernant les faits en cause, et d'une action concertée pour nuire à la capacité de l'enquête d'établir la responsabilité des personnes concernées.

Concernant les manquements imputés à la police de Trabzon, la Cour relève que l'ordonnance de non-lieu rendue par le parquet de Trabzon était basée sur des arguments contredits par d'autres éléments du dossier. En particulier, le parquet a estimé que les policiers n'avaient pas jugé convaincants les renseignements qu'ils avaient reçus sur le projet d'assassinat, alors qu'en réalité les policiers avaient informé la police d'Istanbul de l'imminence de l'assassinat. De plus, le classement sans suite des accusations contre le chef de la police ne reposait sur aucune investigation. Globalement, l'enquête du parquet se résument plutôt à une défense des policiers, sans apporter d'éléments sur la question de leur inactivité face aux auteurs présumés de l'assassinat.

Concernant les manquements imputés à la police d'Istanbul, la Cour constate qu'aucune poursuite pénale n'a non plus été déclenchée, en dépit des conclusions des inspecteurs du ministère de l'Intérieur, selon lesquels les responsables de la police n'avaient pas pris les mesures exigées par la situation. La question de savoir pourquoi la police d'Istanbul n'a pas réagi à la menace n'a pas été élucidée.

La Cour reconnaît qu'une action pénale est toujours en cours contre les auteurs supposés de l'attentat. Elle ne peut cependant que relever que toutes les poursuites mettant en cause la responsabilité des autorités officielles ont été classées sans suite (sauf celle engagée contre deux sous-officiers de Trabzon, ce qui n'altère toutefois pas la conclusion de la Cour).

Enfin, la Cour relève que les enquêtes visant la gendarmerie de Trabzon et la police d'Istanbul ont été menées par des fonctionnaires faisant partie de l'exécutif, et que les proches du défunt n'ont pas été associés aux procédures, ce qui affaiblit les enquêtes menées. Les soupçons selon lesquels l'un des chefs de la police aurait soutenu les agissements des accusés ne paraissent pas non plus avoir fait l'objet d'une enquête approfondie.

L'article 2 a donc été violé (sous son « volet procédural »), aucune enquête effective n'ayant été menée s'agissant des défaillances dans la protection de la vie de Fırat Dink.

Grief relatif à la liberté d'expression de Fırat Dink (article 10)

Le Gouvernement turc soutenait que Fırat Dink n'était pas victime d'une atteinte à sa liberté d'expression car, au moment de son décès, aucune condamnation définitive n'avait été prononcée contre lui. La Cour souligne cependant que lorsque Fırat Dink est décédé, la plus haute instance pénale avait confirmé qu'il était coupable d'avoir dénigré la turcité. Qui plus est, ce constat avait fait de lui une cible pour les milieux ultranationalistes et les autorités turques, informées du projet d'assassinat à son encontre, n'ont pas pris de mesures pour le protéger. Il y a, dès lors, eu une ingérence dans l'exercice Fırat Dink de sa liberté d'expression. Selon la jurisprudence de la Cour, une telle ingérence est acceptable si elle est prévue par la loi, si elle poursuit un « but légitime » et si elle peut passer pour avoir été « nécessaire dans une société démocratique ». La Cour doute qu'il ait été satisfait aux deux premiers critères, mais concentre son raisonnement sur le troisième.

Comme le procureur général près la Cour de cassation, elle estime que l'examen de l'ensemble de la série d'articles dans laquelle Fırat Dink avait utilisé l'expression contestée fait clairement apparaître que ce qu'il qualifiait de « poison » n'était pas le « sang turc » comme l'a jugé la Cour de cassation, mais la « perception du Turc » chez l'Arménien et le caractère « obsessionnel » de la démarche de la diaspora arménienne visant à faire reconnaître par les turcs que les événements de 1915 constituent un génocide. Après avoir analysé la façon dont la Cour de cassation avait interprété et concrétisé la notion de turcité, la Cour conclut qu'en réalité, la Cour de cassation a indirectement sanctionné Fırat Dink pour avoir critiqué le fait que les institutions de l'Etat nient la thèse du génocide quant aux

incidents de 1915. Or, la Cour rappelle que l'article 10 de la Convention ne permet pas de restrictions à la liberté d'expression dans le domaine du discours politique ou de questions d'intérêt général, et que les limites de la critique admissible sont plus larges à l'égard du gouvernement que d'un simple particulier. Elle retient aussi que l'auteur s'exprimait en tant que journaliste sur une question d'intérêt général. Enfin, elle rappelle que la recherche de la vérité historique fait partie intégrante de la liberté d'expression. La Cour en conclut que condamner Firat Dink pour dénigrement de la turcité ne répondait à aucun « besoin social impérieux ».

En outre, la Cour rappelle que les Etats sont tenus de créer un environnement favorable à la participation aux débats publics de toutes les personnes concernées, leur permettant d'exprimer sans crainte leurs opinions et idées. Dans une telle affaire, l'Etat ne devait pas simplement s'abstenir de toute ingérence dans la liberté d'expression de l'intéressé, mais avait aussi l'« obligation positive » de protéger son droit à la liberté d'expression contre des atteintes provenant même de personnes privées. Vu ses constats concernant le manquement des autorités à protéger Firat Dink contre l'attaque des membres d'un groupe ultranationaliste, et concernant le verdict de culpabilité prononcé sans que cela corresponde à un « besoin social impérieux », la Cour conclut que les « obligations positives » qu'avait la Turquie au regard de la liberté d'expression de Firat Dink n'ont pas été respectées.

L'article 10 a donc été violé.

Grief relatif à l'absence alléguée de recours effectif (article 13 combiné avec l'article 2)

Dans les affaires concernant le droit à la vie, l'article 13 exige non seulement le versement d'une indemnité le cas échéant, mais aussi des investigations approfondies et effectives propres à conduire à l'identification et à la punition des responsables et comportant un accès effectif de la famille à la procédure d'enquête (ce qui va plus loin que l'obligation de mener une enquête effective imposée par l'article 2). L'absence d'enquête pénale effective dans cette affaire amène donc la Cour à constater également une violation de l'article 13 de la Convention combiné avec l'article 2, les requérants ayant été ainsi privés de l'accès à d'autres recours théoriquement disponibles, tels qu'une action en dommages-intérêts.

Satisfaction équitable (mise en œuvre de l'article 41)

La Cour dit que la Turquie doit verser, pour dommage moral, 100 000 euros (EUR) conjointement à la femme et aux enfants de Firat Dink, et 5 000 EUR à son frère. Elle doit en outre verser 28 595 EUR conjointement aux requérants pour frais et dépens.

Le juge Sajó a exprimé une opinion séparée, à laquelle s'est jointe la juge Tsotsoria. Le texte s'en trouve joint à l'arrêt.

Jurisprudence française

N° 91

1^o CRIMES ET DELITS COMMIS A L'ETRANGER

Délit – Poursuite en France – Conditions – Fait puni par la loi étrangère – Constatations nécessaires

2^o CRIMES ET DELITS COMMIS A L'ETRANGER

Délit – Délit commis contre un particulier – Plainte préalable ou dénonciation officielle – Constatations nécessaires

1^o Méconnaît les dispositions de l'article 113-6 du code pénal l'arrêt qui prononce une condamnation à raison de délits de vols aggravés et d'escroqueries, en récidive, commis à l'étranger sans constater que les faits sont punissables par la législation du pays où ils ont été perpétrés.

2^e Aux termes de l'article 113-8 du code pénal, en cas de délit commis à l'étranger, contre un particulier, la poursuite intentée par le ministère public doit être précédée d'une plainte de la victime ou de ses ayants droit ou d'une dénonciation officielle de l'autorité du pays où le fait a été commis.

Dès lors doit être cassé l'arrêt qui ne met pas la Cour de cassation en mesure de s'assurer que les dispositions de cet article, notamment en ce qui concerne la plainte préalable de la victime, ont été respectées.

CASSATION sur le pourvoi formé par X... Grégory, contre l'arrêt de la cour d'appel d'Aix-en-Provence, 13^e chambre, en date du 7 septembre 2009, qui, pour vols aggravés et escroqueries, en récidive, l'a condamné à deux ans d'emprisonnement, et a prononcé sur les intérêts civils.

26 mai 2010

N° 09-86.499

LA COUR,

Vu le mémoire produit ;

Sur le premier moyen de cassation, pris de la violation des articles 113-6, 113-8 du code pénal et 591 du code de procédure pénale :

« en ce que l'arrêt attaqué a déclaré Grégory X... coupable de vols et escroqueries en réunion en état de récidive légale et l'a condamné à une peine de deux ans d'emprisonnement et s'est prononcé sur les intérêts civils après avoir constaté qu'après identification de Grégory X..., les policiers suisses apprenaient qu'il était incarcéré en France (où il purgeait dix-huit mois pour des faits similaires commis en janvier 2006) et dénonçant les faits aux autorités françaises le 2 août 2006 ;

« 1^e alors qu'il résulte de l'article 113-6, alinéa 2, du code pénal, que, lorsqu'un délit est commis par un Français hors du territoire de la République, la loi française n'est applicable que si les faits sont punis par la législation du pays où ils ont été commis ; qu'il ressort de l'arrêt attaqué que Grégory X... a été poursuivi pour soustractions frauduleuses de cartes bancaires et escroqueries commises en Suisse et condamné de ce chef ; qu'en statuant ainsi, sans avoir recherché si le délit retenu à son encontre était également puni par la législation en vigueur au lieu de sa perpétration, les juges ont méconnu le texte précité ;

« 2^e alors qu'il résulte de l'article 113-8 du code pénal, que la poursuite des délits commis à l'étranger par un Français doit être précédée d'une plainte de la victime ou d'une dénonciation officielle de l'autorité

du pays où le fait a été commis ; que la cour d'appel constate que les pièces du dossier établi en Suisse ont été transmises par la police suisse ; que, dès lors que la police n'est pas une autorité au sens de l'article précité, la cour d'appel en a méconnu le sens » ;

Vu les articles 113-6, 113-8 du code pénal, 591 et 593 du code de procédure pénale ;

Attendu que, d'une part, aux termes de l'article 113-6 du code pénal, la loi pénale française « est applicable aux délits commis par des Français hors du territoire de la République si les faits sont punis par la législation du pays où ils ont été commis » ;

Que, d'autre part, l'article 113-8 du même code dispose qu'en cas de délit commis à, l'étranger contre un particulier, la poursuite, qui ne peut être intentée qu'à la requête du ministère public, « doit être précédée d'une plainte de la victime ou de ses ayants droit ou d'une dénonciation officielle par l'autorité du pays où le fait a été commis » ;

Attendu que l'arrêt attaqué déclare Grégoire X..., dont la nationalité française n'est pas mise en cause, coupable des délits de vols aggravés et escroqueries, alors qu'il résulte des constatations des juges du fond que les faits constitutifs de ces délits ont été commis en territoire étranger ;

Qu'il appartenait à la juridiction saisie de rechercher si les délits retenus à la charge du prévenu étaient également punis par la législation en vigueur au lieu de leur perpétration ;

Qu'à défaut d'une constatation à cet égard, la décision a violé l'article 113-6 précité ;

Attendu qu'au surplus, et alors que les délits ont été commis contre des particuliers, le même arrêt laisse incertain le point de savoir si la poursuite, intentée par le ministère public, a été ou non précédée d'une plainte des victimes ou de leurs ayants droit ou d'une dénonciation officielle par l'autorité du pays où ils ont été commis ;

Qu'ainsi la Cour de cassation n'est pas mise en mesure de s'assurer que les dispositions de l'article 113-8 du code pénal ont été respectées ;

Que la cassation est encourue de ces chefs ;

Par ces motifs, et sans qu'il soit besoin d'examiner les autres moyens de cassation proposés :

CASSE et ANNULE, en toutes ses dispositions, l'arrêt susvisé de la cour d'appel d'Aix-en-Provence, en date du 7 septembre 2009, et pour qu'il soit à nouveau jugé, conformément à la loi ;

RENOVOIE la cause et les parties devant la cour d'appel d'Aix-en-Provence, autrement composée, à ce désignée par délibération spéciale prise en chambre du conseil.

*Président : M. Louvel – Rapporteur : M. Straehli – Avocat général :
Mme Magliano – Avocat : SCP Lyon-Caen, Fabiani et Thiriez.*

ASSOCIATION DE MALFAITEURS

Infraction autonome et distincte des délits préparés

Cass. crim., 30 juin 2010, n° 10-80.559, F-D : JurisData n° 2010-014870

(...)

Sur le moyen unique de cassation, pris de la violation des articles 450-1 à 450-5, 313-1, 313-2, 313-3, 313-7, 313-8 du Code pénal ;

Vu les articles 388 et 593 du Code de procédure pénale ;

• Attendu que, d'une part, s'il appartient aux juges répressifs de restituer aux faits dont ils sont saisis leur véritable qualification, c'est à la condition de n'y rien ajouter, sauf acceptation expresse par le prévenu d'être jugé sur des faits non compris dans la poursuite ;

• Attendu que, d'autre part, tout jugement ou arrêt doit comporter les motifs propres à justifier la décision ; que l'insuffisance ou la contradiction des motifs équivaut à leur absence ;

• Attendu qu'il résulte de l'arrêt attaqué que Stelica I., auquel il est reproché d'avoir été à la tête d'un réseau de contrefaçon de cartes bancaires utilisées pour obtenir des espèces et des marchandises, est poursuivi des chefs, notamment, d'association de malfaiteurs en vue de préparer des escroqueries en bande organisée, d'escroqueries et de fabrication, acquisition, détention d'instruments de contrefaçon ;

• Que les juges d'appel, après l'avoir déclaré coupable de ce dernier délit ainsi que d'escroqueries et complicité d'escroqueries « en bande organisée », l'ont relaxé du chef d'association de malfaiteurs au motif que les mêmes faits, tenant à l'existence d'une bande organisée, « ne peuvent être retenus à la fois comme élément constitutif d'un délit et comme circonstance aggravante d'une autre infraction » ;

• Mais attendu qu'en prononçant ainsi alors que, d'une part, la circonstance aggravante de bande organisée n'était pas comprise dans les poursuites pour escroquerie, d'autre part, l'association de malfaiteurs constitue une infraction autonome, distincte des délits préparés, la cour d'appel a excédé les limites de sa saisine et n'a pas justifié sa décision de relaxe ;

D'où il suit que la cassation est encourue ;

Par ces motifs :

Casse et annule,

(...)

ATTEINTES AUX INTÉRêTS FONDAMENTAUX DE LA NATION

TGI Clermont-Ferrand, ch. corr., 21 juin 2010

1^{er} Sur le délit d'abus de confiance

• Attendu que le contrat de travail signé par M. A. le 31 mai 2000 rappelle l'exigence de confidentialité pesant sur les salariés de la Manufacture Michelin ; qu'il s'est de la sorte engagé « à ne donner communication à personne, en dehors des besoins stricts de travail, soit pendant, soit après son séjour dans l'entreprise de toute note ou document concernant la Manufacture et ses opérations et à prendre les dispositions nécessaires pour éviter tout accès non autorisé à ces documents et aux informations qu'ils contiennent » ; que le contrat précise que « tout support sur lequel de telles notes ou copies seraient portés deviendrait immédiatement et resterait la propriété de la Manufacture » ;

• Attendu que l'expertise informatique réalisée par M. L. a mis en évidence que le disque dur de l'ordinateur de M. A. contenait un nombre très important de données concernant la manufacture Michelin ; qu'un volume de 5,2960, soit 2249 dossiers et 13386 fichiers a ainsi pu être recensé ; que l'expert indique que ces données étaient classées dans un répertoire intitulé « Mikowill » contenait des données modifiées ;

• Attendu que M. A. a reconnu qu'il avait collecté ces données informatiques dans le cadre de son activité professionnelle, grâce à l'accès au serveur informatique dont il disposait ; que certaines de ces informations ont été enregistrées au cours de sa période de préavis :

• Attendu qu'il a également admis avoir conservé ces données après la rupture de son contrat de travail, tout en sachant qu'une telle pratique était contraire aux règles de confidentialité existant dans l'entreprise ;

• Attendu qu'en gardant en sa possession des données qu'il savait ne lui être communiqués que pour les besoins de son activité professionnelle et en en faisant usage à des fins totalement étrangères, M. A. s'est rendu coupable du délit d'abus de confiance ;

2^{me} Sur le délit d'atteinte aux intérêts fondamentaux de la Nation

• Attendu que M. A. se voit reproché d'avoir recueilli ou rassemblé, en vue de la livrer à une entreprise étrangère, des renseignements, procédés, objets, documents donnés informatisées ou fichiers, dont l'exploitation, la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la Nation ;

• Attendu qu'il est acquis tout d'abord que M. A. a collecté des éléments d'informations en vue de les communiquer à des entreprises étrangères, en l'occurrence les sociétés Bridgestone, Good Year, et Kuhmo ;

• Attendu cependant d'une part, qu'il apparaît que la démarche de M. A. de s'adresser à ces trois sociétés, était plus dictée par la considération qu'il s'agissait de concurrents directs de la Manufacture Michelin que par celle qu'il s'agissait d'entreprises étrangères ;

• Attendu d'autre part, que s'il est indéniable que les informations rassemblées par M. A., présentaient un caractère de confidentialité important, de sorte que leur divulgation à une entreprise concurrente était de nature à porter atteinte à la stratégie commerciale de l'entreprise Michelin, il n'en résulte pas pour autant que M. A. ait également porté atteinte aux intérêts fondamentaux de la Nation ;

• Attendu que l'article 410-1 du Code pénal précise que les intérêts fondamentaux de la Nation s'entendent de l'intégrité de son territoire, de sa sécurité, de la forme républicaine de ses institutions, des moyens de sa défense et de sa diplomatie, de la sauvegarde de sa population, 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 culturel ;

• Or attendu qu'en l'état des éléments techniques recueillis au cours de l'instruction, il ne peut être tenu pour établi que les

informations recueillies par M. A. dans le cadre de son activité professionnelle au sein de la Manufacture M., présentaient un caractère à ce point stratégique qu'elle mettaient en jeu des éléments essentiels du potentiel économique français.

• Attendu que si le centre de recherche de Ladoix de la Manufacture Michelin fait l'objet d'un classement comme Établissement à régime restrictif (ERR), conformément aux termes de l'instruction interministérielle du 1^{er} mars 1993, il n'est pas démontré que les données informatiques en possession de M. A. concernaient des recherches effectuées sur ce site ; qu'au demeurant, le seul fait du classement en ERR n'induit pas nécessairement que des éléments essentiels du potentiel économique de la France, au sens de l'article 410-1 du Code pénal, soient concernés.

• Attendu que les éléments constitutifs de l'infraction prevue par l'article 411-7 du Code pénal n'apparaissent en définitive pas caractérisés, qu'une relaxe doit être prononcée de ce chef :

3^{me} Sur le délit de violation de secrets de fabrique

• Attendu qu'il est reproché à M. A., étant salarié de l'entreprise Michelin, d'avoir révélé ou tenté de révéler un secret de fabrique.

• Attendu que l'ordonnance de renvoi considère que constitue un tel secret, le contenu de l'un des échantillons répertorié sous l'appellation « other sample » relatif à un mélange connu sous le code de « Gin's » ;

• Attendu cependant que ne figure que dossier d'information, aucun élément technique suffisamment objectif, émanant en particulier d'autres personnes que des salariés de la Manufacture Michelin, permettant d'affirmer que ce mélange Gin's constituait effectivement un procédé de fabrication particulier offrant un intérêt pratique ou commercial, tenu secret ; qu'aucune précision n'a également été apportée par la Manufacture Michelin concernant le dépôt d'éventuel brevet pour ce procédé qui était déjà en phase de développement ;

• Attendu que le délit reproché à M. A. à ce titre apparaît insuffisamment caractérisé ; qu'une relaxe doit donc être prononcée ;

B. - Sur la peine

• Attendu que même si une relaxe a été prononcée sur deux des trois chefs de prévention, il demeure que le comportement de M. A. présente une incontestable caractére de gravité ;

• Attendu en effet que l'information a permis de mettre en évidence qu'il avait conçu un plan d'action méthodique et détaillé, afin de monnayer les nombreuses informations qu'il avait pris soin de collecter, notamment durant les derniers mois, de son activité au sein de la Manufacture Michelin ; que le caractère parfaitement réfléchi et planifié de son action rend peu crédible l'explication avancée tout au long de l'information selon laquelle il s'agissait d'un jeu pervers né du désœuvrement ;

• Attendu que M. A., qui a indiqué vouloir tester son pouvoir de nuisance à l'égard de son ancien employeur, a de plus incontestablement agi avec l'intention de nuire à la Manufacture Michelin ;

• Attendu que ces faits doivent être sanctionnés par une peine d'emprisonnement d'une durée significative qui sera fixée à deux ans ; que l'absence de tout antécédent judiciaire de l'intéressé justifie d'assortir intégralement cette peine du sursis simple ;

• Attendu qu'une amende de 5 000 euros sera également prononcée ;

II - Sur l'action civile

• Attendu que pour incontestable qu'il soit, le préjudice subi par la Manufacture Michelin, du fait des agissements de son ancien salarié, est malgré tout demeuré limité puisque les informations détournées par M. A. n'ont pas été effectivement portées à la connaissance de ses concurrents ; qu'une indemnité de 10 000 euros réparera ce préjudice ;

• Attendu qu'une indemnité de 2 000 euros sera également allouée à la Manufacture Michelin au titre de l'article 475-1 du Code de procédure pénale ;

Par ces motifs

Le tribunal, statuant publiquement, en premier ressort et contradictoirement à l'égard de M. A., contradictoirement à l'égard de la Manufacture française de pneumatiques Michelin,

Sur l'action publique :

- Renvoie M. A. des fins de la poursuite concernant le délit d'atteinte aux intérêts fondamentaux de la Nation et de violation des secrets de fabrique ;

- Le déclare coupable du délit d'abus de confiance ;

Condamne M. A. à un emprisonnement délictuel de deux ans ;
Vu l'article 132-31 alinéa 1 du Code pénal ;
Dit qu'il sera sursis totalement à l'exécution de cette peine, dans
les conditions prévues par ces articles ;
Dit que l'avertissement prévu par l'article 132-29 du Code pénal
sera donné par Madame la Présidente au condamné en fonction de
sa présence à l'audience lors du prononcé du délibéré ;
- Condamne M. A.
(...)

Propositions de lois

Dans le cadre de l'examen de la proposition de loi de simplification et d'amélioration de la qualité du droit par la Commission des lois du Sénat, deux amendements ont été présentés par Messieurs SUEUR et YUNG, Madame KLES, Monsieur FRIMAT et les membres du groupe socialistes, apparentés et rattachés relatifs à une modification des articles 13 et 20 de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques. Ces deux amendements ont été rejetés le 06 octobre 2010 par la Commission des lois du Sénat.

N° COM – 139 04/10/10

Article additionnel avant article 29

Avant l'article 29, insérer l'article suivant :

L'article 13 de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques est ainsi modifié :

La troisième phrase du premier alinéa est complétée comme suit :

Et de l'article 20.

Objet

Cet amendement a pour objet d'étendre le contrôle de la CNCIS aux mesures de surveillance et de contrôle des transmissions empruntant la voie hertzienne, prises par les pouvoirs publics aux seules fins de défense des intérêts nationaux (article 20 de la loi du 10 juillet 1991).

Par nature et pour raisons techniques, l'article 20 de la loi du 10 juillet 1991 a été, dès l'origine, exclu du champ d'application de la loi sur le contrôle des interceptions de sécurité.

Or, l'article 20, dans sa rédaction en vigueur, comporte des subtilités sémantiques qui peuvent être interprétées de manière différente au point de pouvoir contredire la volonté du législateur de concilier deux objectifs essentiels ; ne pas désarmer l'Etat face à un certain nombre de menaces comme le terrorisme, tout en offrant des garanties réelles à la protection des libertés individuelles.

L'extension à la CNCIS du contrôle des interceptions relevant de l'article 20 de la loi du 10 juillet 1991 permettrait de lever toutes les

ambiguïtés sur l’application du dispositif en évitant que les agents habilités des services compétents du ministère de la Défense et du ministère de l’Intérieur puissent s’adresser directement auprès des opérateurs sans en référer préalablement à la CNCIS.

En favorisant la lisibilité de la loi du 10 juillet 1991, le présent amendement participe à la démarche d’amélioration de la qualité du droit sur un sujet qui intéresse la défense des intérêts de la nation des libertés individuelles

N° COM – 140 du 04/10/2010

Article additionnel avant article 29

Avant l’article 29, insérer l’article suivant :

L’article 20 de la loi N° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques est ainsi modifié :

1°) remplacer le mot « empruntant » par les mots « qui ne sont pas individualisables, localisées et quantifiables et qui empruntent... »

2°) compléter cet article par les mots : « sous réserve des dispositions de l’article 13 ».

Objet

L’article 20 de la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques exclut du contrôle de la légalité des autorisations d’interceptions de sécurité «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».

On peut considérer, sans qu’il soit nécessaire de le préciser explicitement, que cette disposition interdit les services compétents de relever de données de connexion ou de procéder à des écoutes individuelles et localisées et encore moins de consulter la facture téléphonique détaillée d’un abonné individualisé dans le cadre de cette disposition.

En effet, cette dernière ne concerne que les opérations de balayage des fréquences radioélectriques réalisées dans le cadre de la mission générale de défense des intérêts nationaux confiée aux pouvoirs publics à l’occasion desquelles peuvent être interceptées, de manière aléatoire, des communications le plus souvent codées.

A l'exception de ce cas précis, les interceptions doivent pouvoir être contrôlées selon la procédure d'autorisation codifiée à l'article 4 de la loi du 10 juillet 1991.

Or, en pratique, cette disposition dérogatoire peut se prêter à une mauvaise interprétation et laisser penser qu'elle autoriserait l'interception d'un numéro déterminé et la consultation des relevés de communication sans autorisation préalable.

Afin de lever toute ambiguïté sur le champ d'application de l'article 20 de la loi du 10 juillet 1991, les auteurs de l'amendement proposent de sortir de l'obscuré clarté rédactionnelle de cette disposition en précisant que les opérations d'interception auxquelles elle s'applique ne sauraient viser les communications individualisables, localisées et quantifiables.

Sans cette dernière précision, de telles interceptions dérogatoires au droit commun défini par la loi du 10 juillet 1991 deviendraient sauvages et constitutives d'une ingérence de l'autorité publique dans l'exercice par toute personne de son droit au respect de sa correspondance.

Table des matières

Avant propos	5
Première partie	
RAPPORT D'ACTIVITÉ	7
Chapitre I	
Organisation et fonctionnement de la Commission	9
Composition de la Commission	9
Rappel des compositions successives de la Commission	10
Missions et fonctionnement	11
Financement.....	12
Relations extérieures.....	13
Chapitre II	
Le contrôle des interceptions de sécurité (loi n° 91-646 du 10 juillet 1991).....	15
Le contrôle des autorisations	15
Le contrôle de l'exécution.....	26
Le contrôle du matériel	30
Chapitre III	
Le contrôle des opérations de communication des données techniques en matière de prévention du terrorisme (loi n° 2006-64 du 23 janvier 2006)	33
Présentation du dispositif	35
Eléments d'ordre statistique.....	36
Etendue et modalités du contrôle exercé par la CNCIS	40

Deuxième partie	
JURISPRUDENCE DE LA COMMISSION.....	43
La qualité de la motivation des demandes d'interception.....	45
Sécurité nationale.....	46
Sauvegarde des éléments essentiels du potentiel scientifique et économique de la Nation.....	49
Prévention du terrorisme	52
Prévention de la criminalité et de la délinquance organisées	54
Troisième partie	
ÉTUDES ET DOCUMENTS	59
Chapitre I	
Présentation ordonnée des textes relatifs aux missions de la Commission	61
Première mission : les interceptions	61
Deuxième mission : les opérations de communications de données techniques (loi 2006-64 du 23 janvier 2006)	75
Troisième mission : le contrôle du matériel	78
Chapitre II	
Interceptions de sécurité et secret-défense	89
Chapitre III	
Éléments de jurisprudence et actualités parlementaires.....	93
Jurisprudence européenne	93
Jurisprudence française.....	105
Propositions de lois	113