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 nº 91-646 du 10 juillet 1991) 13

Chapitre III
Le contrôle des opérations de communication des données techniques (loi nº 2006-64 du 23 janvier 2006) 29

Deuxième partie
JURISPRUDENCE DE LA COMMISSION 33

Troisième partie
ÉTUDES ET DOCUMENTS 53

Chapitre I
Présentation ordonnée des textes relatifs aux missions de la Commission 55

Chapitre II
Actualité législative et réglementaire 81

Chapitre III
Interceptions de sécurité et secret-défense 91

Chapitre IV
Jurisprudence des cours et tribunaux 93

Chapitre V
Questions parlementaires 109

Table des matières 111

Information au lecteur : les rapports d'activité de la CNCIS auxquels il est parfois renvoyé dans les pages qui suivent sont accessibles en ligne (à partir du rapport 2000) sur le site de La Documentation française www.ladocumentationfrançaise.fr (rubrique « Bibliothèque des rapports publics »).

Avant-propos

L'année 2007 aura été fertile en événements en ce qui concerne la Commission.

Tout d'abord, une Commission renouvelée a été mise en place. Suite au décès brutal du sénateur Jacques Baudot auquel je tiens à rendre ici hommage, le président du Sénat a désigné Monsieur Hubert Haenel, sénateur du Haut-Rhin, ancien magistrat, maître des requêtes (h) au Conseil d'État, comme membre de la Commission. Puis, le président de l'Assemblée nationale a désigné, au lendemain des élections législatives, Monsieur Daniel Vaillant, député de Paris, ancien ministre de l'Intérieur, comme l'autre membre de la Commission. Ce sont deux hommes politiques de grande expérience qui sont ainsi venus m'épauler et je m'en réjouis.

À peu près à la même période, le délégué général Gérard Lorho quittait la Commission pour reprendre le cours de sa carrière de magistrat. Il était immédiatement remplacé dans cette fonction par Rémi Récio, précédemment chargé de mission. La Commission était enfin à nouveau au complet début novembre, avec l'arrivée de François Coudert, nouveau chargé de mission.

Ces changements de personnel, tant au niveau politique qu'au niveau des agents n'ont pas ralenti notre activité, comme cela ressort du chiffre total des interceptions de sécurité accordées (6 000 contre 5 985 en 2006), ainsi que des autres paramètres statistiques. Surtout, l'année 2007 a vu la « montée en régime », à compter du 1er mai, de la structure dirigée par la « personnalité qualifiée » désignée par la Commission en application de l'article 6 de la loi antiterroriste du 23 janvier 2006, à savoir l'inspecteur général François Jaspart. Ce sont ainsi plus de 25 982 « données techniques » d'identification ou de connexion qui ont été demandées aux opérateurs et aux hébergeurs par les services habilités après autorisation de la personnalité qualifiée. Bien qu'exercée *a posteriori* – et non *a priori* comme en matière d'interceptions de sécurité – la tâche de contrôle par

la Commission des décisions de la « personnalité qualifiée » est venue s'ajouter à une activité déjà soutenue pour une petite institution comme la nôtre, en cours de réorganisation.

* * *

L'actualité politique et économique de cette année 2007, tant sur le plan national qu'international, dans les domaines intéressant l'activité de la Commission, aura été l'occasion d'un réexamen de certaines de nos jurisprudences, qui ont pu ainsi être nuancées ou enrichies. Ceci sera exposé dans le chapitre du rapport consacré aux « motifs » prévus par la loi du 10 juillet 1991. Nous avons également conduit une réflexion sur la qualité de la motivation des demandes d'interceptions de sécurité, dont le caractère inégal – selon les services et les périodes – a entraîné une augmentation sensible du nombre « d'observations ». La Commission voudrait rappeler ici, avec une certaine solennité, que pour exercer correctement la mission qui lui a été confiée par le législateur, elle doit disposer de demandes dont la motivation est *suffisante*, *pertinente*, et bien entendu *sincère.* Ce point sera développé, dans la partie (nouvelle) du rapport de la Commission, consacrée à l'explicitation de sa « jurisprudence ».

C'est à l'aune de cette appréciation, qui continue de s'appuyer sur les principes de proportionnalité et de subsidiarité, que la Commission poursuit sa tâche, dans le même esprit de dialogue qui l'animait jusqu'à présent, ce qui n'exclut pas dans certains cas une sévérité quelque peu accrue. La balance à tenir entre la protection des libertés individuelles et la sécurité publique est à ce prix.

Jean-Louis DEWOST
Président de la Commission

Première partie

RAPPORT D'ACTIVITÉ

Chapitre I

Organisation et fonctionnement de la Commission

Composition de la Commission

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

Membres de la Commission :

• Président : Jean-Louis Dewost, président de section honoraire au Conseil d'État nommé pour une durée de six ans par le Président de la République (décret du 29 septembre 2003, publié au *Journal officiel* le 30 septembre 2003).

• Membre parlementaire – Sénat : Hubert Haenel, sénateur (UMP) du Haut-Rhin, désigné le 4 juillet 2007 par le président du Sénat.

• Membre parlementaire – Assemblée nationale : Daniel Vaillant, député (PS) de Paris, désigné le 1er août 2007 par le président de l'Assemblée nationale.

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

• Rémi Récio, délégué général depuis sa nomination en date du 2 mai 2007.

• François Coudert, chargé de mission depuis sa nomination en date du 5 novembre 2007,

Le secrétariat est assuré par Mesdames Nathalie Brucker et Françoise Nudelmann.

Monsieur Christophe Germin conduit le véhicule de la Commission.

Rappel des compositions successives de la Commission

• Présidents

• Paul Bouchet, conseiller d'État, 1er octobre 1991.
• Dieudonné Mandelkern, président de section au Conseil d'État, 1er octobre 1997.
• Jean-Louis Dewost, président de section au Conseil d'État, 1er octobre 2003.

• Représentants de l'Assemblée nationale

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

• Représentants du Sénat

• Marcel Rudloff, sénateur du Bas-Rhin, 17 juillet 1991.
• Jacques Thyraud, sénateur du Loir-et-Cher, 26 mars 1992.
• Jacques Golliet, sénateur de Haute-Savoie, 22 octobre 1992.
• Jean-Paul Amoudry, sénateur de Haute-Savoie, 14 octobre 1995.
• Pierre Fauchon, sénateur du Loir-et-Cher, 18 septembre 1998.
• André Dulait, sénateur des Deux-Sèvres, 6 novembre 2001.
• Jacques Baudot, sénateur de Meurthe-et-Moselle, 26 octobre 2004.
• Hubert Haenel, sénateur du Haut-Rhin, 4 juillet 2007

Missions et fonctionnement

La Commission est chargée de veiller au respect des dispositions du titre II (« Des interceptions de sécurité ») de la loi no 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, modifiée à plusieurs reprises, la dernière fois par la loi no 2006-64 du 23 janvier 2006.

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

En application de l'article 15 de la loi, la Commission reçoit les réclamations des particuliers, procède en toute indépendance aux contrôles et enquêtes qui lui paraissent nécessaires à l'accomplissement de sa mission et s'attache à nouer tous contacts utiles à son information ; elle peut à tout moment adresser au Premier ministre une recommandation tendant à ce qu'une interception soit interrompue.

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

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

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

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

Financement

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

Pour l'année 2007 et conformément à la déclinaison en programmes, actions et sous-actions de la loi organique relative aux lois de finances, le budget de la CNCIS a été inscrit au sein du programme 129 – Coordination du travail gouvernemental – Action 08 – **Défense et protection des libertés** – où la Commission est regroupée avec la Commission consultative du secret de la défense nationale (CCSDN) et la Commission nationale de déontologie de la sécurité (CNDS).

Afin de respecter l'indépendance budgétaire de ces trois autorités indépendantes, chacune a été dotée d'un budget opérationnel de programme (BOP), celui de la CNCIS étant référencé 129AIC. Les crédits alloués en 2007 se sont élevés à 565 265 euros dont 489 265 euros pour les dépenses du titre II (« Dépenses de personnel ») et à 76 000 euros pour les dépenses de fonctionnement.

Une partie des crédits de personnel est destinée à permettre à la Commission de faire face aux charges nouvelles de contrôle induites par l'article 6 de la loi no 2006-64 du 23 janvier 2006 dont les effets ne peuvent encore être pleinement appréhendés, ce dispositif n'ayant débuté qu'au début du mois de mai 2007.

Les crédits du BOP CNCIS sont destinés en priorité à permettre le fonctionnement continu de la CNCIS en toute sécurité. La structure permanente de la Commission comprend à cet effet outre le président, deux magistrats et deux secrétaires fonctionnant en binômes. La Commission doit pouvoir être jointe et s'entretenir avec ses interlocuteurs de façon sécurisée. Ses locaux sont équipés pour répondre aux normes relatives au traitement des documents estampillés secret-défense. La Commission doit disposer des moyens d'information les plus larges comme les plus spécialisés en source ouverte (presse et documentation). Elle doit également disposer d'un moyen 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.

Les crédits de personnel et de fonctionnement alloués permettront, difficilement pour ce qui concerne le fonctionnement, de répondre à ces priorités, eu égard aux charges nouvelles constatées et prévisibles.

Le contrôle des interceptions de sécurité (loi nº 91-646 du 10 juillet 1991)

Le contrôle des autorisations

Le contrôle en amont

Théorie et pratique

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

La loi de 1991 avait prévu un contrôle *a posteriori*. Toutefois, dès les premiers mois de son fonctionnement, la Commission a instauré avec l'accord du Premier ministre, la pratique du contrôle préalable à la décision d'autorisation allant ainsi au-delà de la lettre de l'article 14 de la loi du 10 juillet 1991. Ce contrôle *a priori* permet un dialogue utile avec les services demandeurs et une meilleure prise en compte par ceux-ci, dès le stade préparatoire, des éléments de la « jurisprudence » de la Commission grâce au relais centralisé que constitue le Groupement interministériel de contrôle (GIC).

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

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

Contrôle formel et respect des contingents

L'activité de contrôle comporte en premier lieu un aspect formel qui consiste à vérifier que les signataires des demandes d'autorisation ont bien été habilités par les ministres compétents. Devant la multiplication des demandes urgentes et afin de fluidifier les procédures, la Commission a suggéré et obtenu que la loi no 2006-64 du 23 janvier 2006 introduise à l'article 4 de la loi du 10 juillet 1991 une nouvelle disposition autorisant chaque ministre, à l'instar du Premier ministre, à déléguer de façon permanente sa signature à deux personnes.

Il convient de rappeler que les contingents d'interceptions simultanées ne doivent pas être confondus avec le nombre total d'interceptions (demandes initiales et renouvellements) réalisées annuellement au profit des trois ministères concernés, Intérieur, Défense et Budget. Dans son souci de conserver un caractère exceptionnel aux interceptions de sécurité, le législateur de 1991 a en effet opté pour une limitation sous forme d'un encours maximum, protecteur des libertés publiques. Ce système déjà mis en place par la décision du 28 mars 1960 du Premier ministre Michel Debré, mais résultant à l'époque considérée de contraintes techniques (capacité maximale d'enregistrement sur des magnétophones à bandes ou à cassettes et capacité d'exploitation par le GIC) a été consacré en 1991 comme devant *« inciter les services concernés à supprimer le plus rapidement possible les interceptions devenues inutiles, avant de pouvoir procéder à de nouvelles écoutes »* (CNCIS, *3e rapport 1994*, p. 16).

Le système par lequel les interceptions sont contingentées – leur nombre doit à tout moment respecter un plafond fixé par ministère en vertu d'une décision du Premier ministre, la répartition interne entre services étant du ressort de chaque ministère – conduit à ce que **le nombre des interceptions à un instant donné est toujours inférieur au contingent** : les services doivent en effet se réserver la possibilité de répondre en permanence à des circonstances inattendues ou à des besoins nouveaux.

L'augmentation constante du parc de vecteurs de communications électroniques (téléphone fixe, mobile, fax, Internet) a conduit à des relèvements progressifs du contingent (50 % depuis l'origine) à rapprocher du doublement du seul parc téléphonique au cours de la même période (1996-2007).

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

Tableau récapitulatif

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

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

Le premier et le seul objectif des interceptions de sécurité est comme leur nom l'indique, la protection de la sécurité de la Nation et de ses intérêts fondamentaux. Les motifs prévus par la loi du 10 juillet 1991, directement inspirés du livre IV du Code pénal qui incrimine les atteintes à ces intérêts fondamentaux, ne font que décliner les différents aspects de la sécurité, mais la référence précise à ceux-ci permet une première appréciation des demandes. Ces motifs, énumérés à l'article 3 de la loi, sont : la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées. Les services demandeurs doivent donc faire référence explicite à l'un de ces motifs légaux. Ils doivent en outre justifier leur demande par des explications circonstanciées qui permettront à la Commission d'apprécier l'articulation du fait au droit. À cet effet la présentation des éléments de fait doit être certes synthétique mais non stéréotypée et suffisamment consistante pour apprécier leur adéquation avec le motif légal. Ce point ainsi que les critères d'appréciation des motivations seront repris dans la deuxième partie du rapport, consacré à la « jurisprudence de la Commission ».

À cet effet le cadre des imprimés de demandes a été revu courant 2006 pour tendre à partir des modèles les plus complets à une uniformisation de la présentation gage d'une meilleure égalité d'appréciation. La Commission attache du prix au caractère exhaustif des mentions notamment relatives aux interceptions précédentes ayant pu exister sur la même cible. Ces cadres ne doivent pas pour autant être perçus comme

un carcan dont on ne pourrait sortir, par exemple en présentant spontanément des informations complémentaires indispensables à l'appréciation de la demande.

Le contrôle s'attache d'une part à une identification aussi précise que possible des cibles, d'autre part aux informations recueillies sur leur activité socioprofessionnelle : il convient en effet de protéger plus particulièrement les professions ou activités jugées sensibles en raison du rôle qu'elles jouent dans une société démocratique (avocats ou journalistes par exemple).

Il importe aussi de s'assurer que le motif légal invoqué ne dissimule pas d'autres préoccupations. Il est nécessaire de rappeler que l'interception doit être sollicitée exclusivement pour les faits articulés et non pour une raison autre qui ne relèverait d'aucun motif légal, quelle que soit par ailleurs la véracité des faits rapportés. Ceci sera développé dans la deuxième partie du rapport.

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

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 son avis. Il formule également les observations qu'il juge utiles sur la pertinence du motif invoqué, procédant le cas échéant à des propositions de 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 ou par des demandes de bilans circonstanciés avant aval d'une nouvelle prolongation dans le cas d'une interception déjà plusieurs fois renouvelée. Il faut enfin veiller à ce que soit respecté le **principe de subsidiarité** et, par conséquent, s'assurer que le but recherché ne puisse être aussi bien rempli par d'autres moyens (enquête de terrain, d'environnement, mise en place de forces de l'ordre, etc.).

Le contrôle en aval

Données chiffrées et commentaires

Évolutions 2006/2007

6 065 interceptions de sécurité ont été sollicitées en 2007 (4 215 interceptions initiales et 1 850 renouvellements). Le caractère inchangé du contingent depuis juin 2005 explique cette quasi-stabilité par rapport à 2006.

S'agissant des interceptions initiales, 964 de ces 4 215 demandes ont été présentées selon la procédure dite d'urgence absolue soit 23 % de ces demandes (17 % en 2006). Il convient ici de préciser que 524 de ces 964 « urgences absolues » ont été constituées d'urgences techniques soit 54,5 % des urgences (32 % en 2006). Force est de constater que ce dernier dispositif permet d'éclairer l'augmentation du nombre de demandes présentées en « urgence absolue ».

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

Cette augmentation constante des urgences absolues pèse de manière significative sur l'organisation de la Commission qui assure un contrôle *a priori* de ces demandes selon une permanence de type parquet. L'un des objectifs prioritaires de cette permanence et de traiter chaque demande d'urgence absolue dans un délai inférieur à une heure. Durant l'année 2007, la Commission a toujours respecté cet objectif.

Au final, si l'on impute à ce chiffre global des demandes d'interceptions (4 215 initiales et 1 850 renouvellements) les 68 avis négatifs donnés par la Commission (44 lors des demandes initiales et 24 lors des demandes de renouvellements) dont 65 ont été suivis par le Premier ministre, ce sont donc 6 000 interceptions de sécurité qui ont effectivement été pratiquées au cours de l'année 2007.

À titre de comparaison, on a dénombré environ 20 000 interceptions judiciaires au cours de la même période.

Pour ce qui concerne les motifs au stade des demandes initiales, c'est toujours la criminalité organisée qui reste le premier motif des demandes initiales avec 56,5 % du total (contre 52 % en 2006) suivie de la prévention du terrorisme avec 31 % (contre 32 % en 2006) et la sécurité nationale 11,5 % (contre 15 % en 2006). Pour ce qui concerne les renouvellements, on note que c'est la sécurité nationale qui occupe la première place avec

43 %, suivie de la prévention du terrorisme avec 42 % et de la criminalité et de la délinquance organisées avec 13,5 %.

Au total, demandes initiales et renouvellements confondus, c'est la prévention de la criminalité organisée qui, cette année encore, se détache nettement avec 43,4 %, suivi de la prévention du terrorisme avec 34,2 % et la sécurité nationale avec 21 %. Ces trois motifs représentent 98,6 % du total des demandes.

Observations

La Commission ayant poursuivi sa démarche de dialogue avec les services demandeurs afin d'aboutir à une logique d'avis moins binaire (avis favorable/avis défavorable), le nombre d'observations a encore crû passant de 745 en 2006 à 1 090 en 2007 dont 139 demandes de renseignements complémentaires et 258 limitations de la durée d'interception sollicitée. Les avis défavorables, comptés dans les observations, sont à nouveau en hausse : 68 (44 lors des demandes initiales et 24 lors des renouvellements) dont 65 ont été suivis par le Premier ministre.

Par ailleurs, les renseignements complémentaires demandés ont conduit les services à ne pas donner suite à trois demandes.

Force est également de constater que le contrôle en amont des demandes, aussi minutieux et exhaustif soit-il, ne saurait suffire. Le contrôle des « productions » (transcription des interceptions) est, en aval, le moyen privilégié pour s'assurer à la fois de la bonne adéquation de la demande au motif légal invoqué et de l'intérêt réel présenté par l'interception au regard des critères de proportionnalité et de subsidiarité. Ce « contrôle continu » inauguré en 2005 s'effectue de manière aléatoire ou ciblée. Il permet ainsi à la Commission, en dépit de la charge matérielle qu'il génère, de prendre des décisions plus éclairées au stade du renouvellement de l'interception s'il est demandé par le service, et le cas échéant, de prendre en cours d'exploitation d'une interception, une recommandation tendant à l'interruption de cette dernière.

Ainsi, les « productions » (transcriptions) de 108 lignes interceptées en 2007 ont elles été examinées et la Commission a recommandé la cessation d'interception de neuf lignes. Elle a été suivie dans tous les cas par le Premier ministre.

Au total avec 6 000 interceptions accordées contre 5 985 en 2006, on constate à nouveau que les interceptions de sécurité demeurent, au regard du nombre des vecteurs de communications électroniques en constante augmentation, la mesure d'exception voulue par la loi. Ce caractère exceptionnel est d'autant plus accusé que chaque vecteur intercepté compte pour une interception quel que soit le nombre de vecteurs utilisés par la cible.

Tableaux annexes

Les demandes initiales d'interception

État des demandes initiales d'interception, années 2006 et 2007

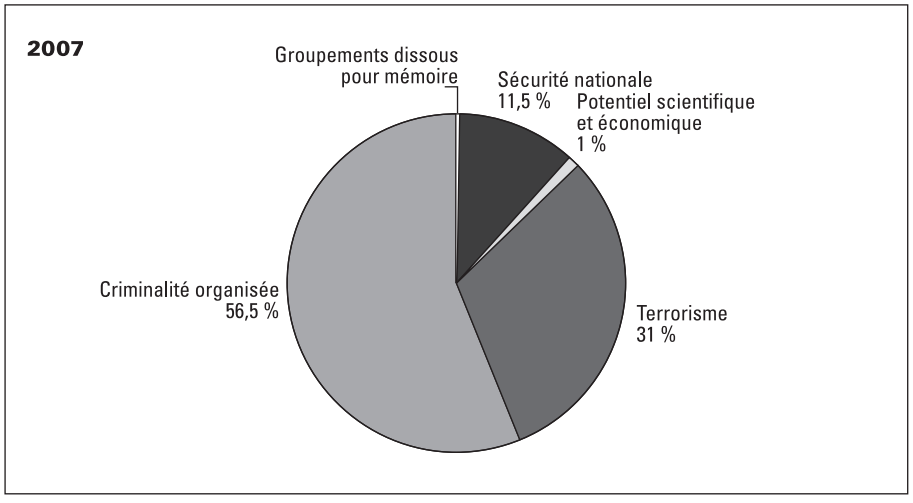
	Demandes initiales		Dont urgence absolue		Accordées	
	Année 2006	Année 2007	Année 2006	Année 2007	Année 2006	Année 2007
Totaux	**4203**	**4215**	**714**	**964**	**4176**	**4173**

État comparatif des demandes initiales sur cinq ans

Motifs	2003	2004	2005	2006	2007
Sécurité nationale	526	548	625	622	479
Potentiel scientifique et économique	42	66	43	47	52
Terrorisme	1126	1292	1468	1330	1295
Criminalité organisée	1668	1881	2006	2195	2381
Groupements dissous	0	0	2	9	8
Totaux	**3362**	**3787**	**4144**	**4203**	**4215**

Demandes initiales

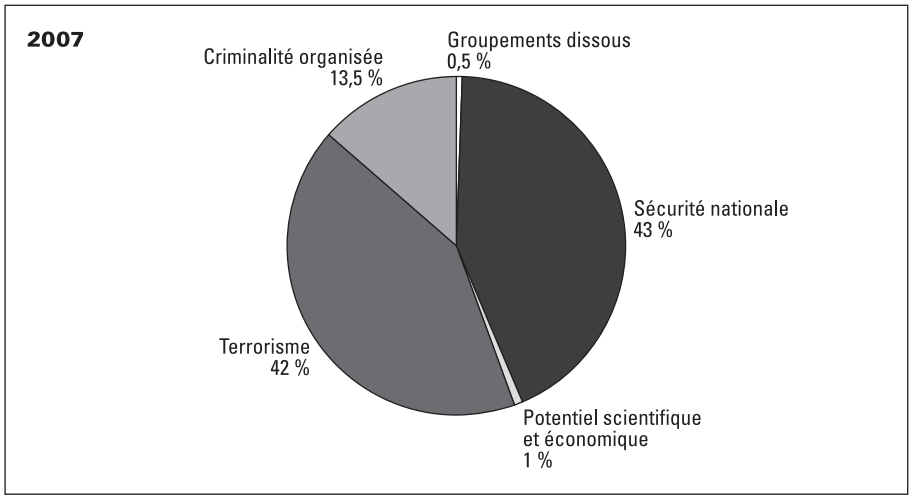
Répartition des motifs



Les renouvellements d'interception

Répartition des motifs en 2007

Sécurité nationale	Potentiel scientifique et économique	Terrorisme	Criminalité organisée	Groupements dissous	Total « demandés »	Total « accordés »
793	20	779	251	7	1 850	1 827



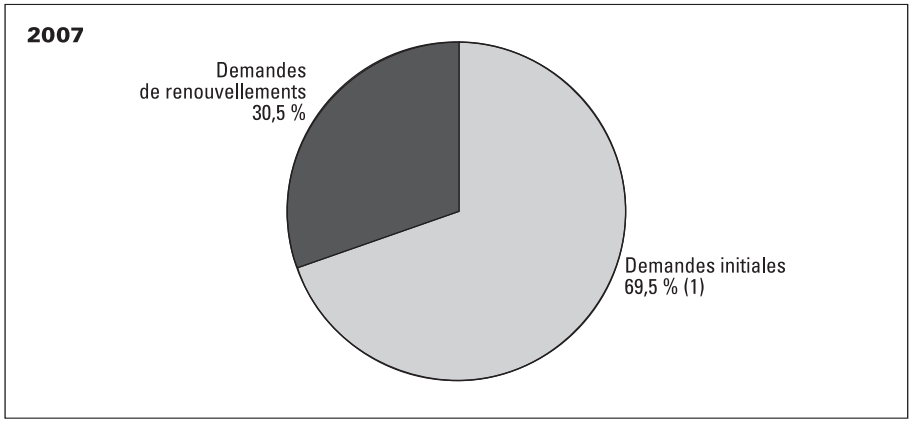
État comparatif des demandes de renouvellements sur cinq ans

Motifs	2003	2004	2005	2006	2007
Sécurité nationale	663	629	624	735	793
Potentiel scientifique et économique	22	36	42	28	20
Terrorisme	782	1 052	848	794	779
Criminalité organisée	210	201	182	243	251
Groupements dissous	0	0	1	9	7
Totaux	**1 677**	**1 918**	**1 697**	**1 809**	**1 850**

Activité globale : demandes initiales et renouvellements

Répartition des demandes entre interceptions et renouvellements d'interceptions

Demandes initiales circuit normal		Demandes initiales en urgence absolue		Demandes de renouvellements	
Année 2006	Année 2007	Année 2006	Année 2007	Année 2006	Année 2007
3489	3251	714	964	1825	1850



(1) Rappel : 23 % des demandes initiales sont constituées par des demandes présentées en urgence absolue.

Demandes d'interceptions : tableau récapitulatif global sur cinq ans

Type de demandes	2003	2004	2005	2006	2007
Demandes initiales d'interceptions	2814	3154	3290	3489	3251
« Urgence absolue »	548	633	854	714	964
Demandes de renouvellements	1677	1936	1738	1825	1850
Total	**5039**	**5723**	**5882**	**6028**	**6065**

Répartition entre interceptions et renouvellements accordés

Interceptions accordées en 2007

Interceptions initiales	Renouvellements	Total
4173	1827	6000

Le contrôle de l'exécution

Celui-ci porte sur trois domaines : en premier lieu, l'enregistrement, la transcription et la durée des interceptions ; en second lieu, les visites sur le terrain ; enfin, l'instruction des réclamations des particuliers et les éventuelles dénonciations à l'autorité judiciaire.

Enregistrement, transcription et destruction

La mise en place en 2002 d'un effacement automatisé de l'enregistrement au plus tard à l'expiration du délai de dix jours, prévu par l'article 9 de la loi, s'est traduite par un gain de temps appréciable pour les agents chargés de l'exploitation. Cette évolution ne dispense cependant pas de l'accomplissement des formalités prévues par le deuxième alinéa de l'article 9 : « Il est dressé procès-verbal de cette opération [de destruction des enregistrements à l'expiration d'un délai de dix jours] ». En application de cette disposition, en début d'année civile, le directeur du GIC atteste de la conformité logicielle du parc informatique de tous ses établissements.

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

Le contrôle du GIC

Service du Premier ministre, consacré comme tel après trente et une années d'existence par le décret no 2002-497 du 12 avril 2002 (CNCIS, *11e rapport 2002*, p. 50) et actuellement dirigé par un officier général, le GIC est l'élément clef du dispositif des interceptions de sécurité. Il en assure la centralisation conformément à l'article 4 de la loi du 10 juillet 1991 (« le Premier ministre organise la centralisation de l'exécution des interceptions autorisées »).

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

Conformément à une recommandation prise par la Commission en 1996, le GIC a entrepris dès 1997 la mise en place de centres locaux de regroupement des interceptions, sortes de GIC déconcentrés répondant aux normes de sécurité souhaitées par la Commission. Cette phase est à ce jour achevée mais le maillage du territoire en antennes secondaires se poursuit attestant, après la nécessaire étape de restructuration centralisée, de la volonté de donner aux services enquêteurs la proximité attendue.

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

Les visites sur le terrain

Comme de coutume la CNCIS a poursuivi son action sur le terrain sous la forme de visites inopinées ou programmées des services utilisateurs d'interceptions.

Lors de ces visites les contrôles portent à la fois sur la sécurisation des locaux, les interceptions en cours, l'examen des relevés d'interception et d'enregistrement (article 8 de la loi) et des procès-verbaux de destruction des enregistrements et des transcriptions (articles 9 et 12 de la loi).

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

Au total, sous une forme ou sous une autre, six visites de services intéressant les régions Nord-Pas-de-Calais, Bretagne, Bourgogne, Rhône-Alpes et Provence-Alpes-Côte-d'Azur ont été effectuées cette année. À chacune de ces visites, les représentants de la CNCIS dressent un inventaire des pratiques et procédures mises en œuvre par les services pour l'application de la loi du 10 juillet 1991, apportent les informations et éclaircissements utiles, notamment sur le rôle de la CNCIS, recueillent les observations des personnels rencontrés sur les matériels et logiciels mis à leur disposition et s'informent des réalités locales se rapportant aux motifs légaux des interceptions.

Réclamations de particuliers et dénonciation à l'autorité judiciaire

Les saisines de la CNCIS par les particuliers

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

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

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

– aucune écoute ou enregistrement permanents des personnels d'une entreprise ou d'une administration ne peut être mis en œuvre sauf législation ou réglementation particulière l'imposant (exemple : passage d'ordres de bourse en salles de marchés) ;

– les écoutes ou enregistrements ponctuels ne sont possibles que dans des cas limités et justifiés (formation du personnel à l'accueil téléphonique par exemple) ;

– l'article L. 120-2 du Code du travail dispose que nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature des tâches à accomplir ni proportionnées au but recherché. L'article L. 121-8 du même Code dispose également qu'aucune information concernant directement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance.

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

S'agissant des courriers adressés à la CNCIS, il leur est immédiatement donné suite et il est notifié au requérant conformément à l'article 17 de la loi que « la Commission a procédé aux vérifications nécessaires ». On relève à ce propos dans les débats parlementaires précédant l'adoption de la loi de 1991 que « *l'imprécision de cette formule…* reprise à l'identique de l'article 39 de la loi du 6 janvier 1978 [loi informatique et libertés] peut sembler insatisfaisante mais il est difficile d'aller plus loin dans la transparence. En effet, à l'occasion de son contrôle, la Commission peut découvrir les situations suivantes :

– existence d'une interception ordonnée par l'autorité judiciaire ;

– existence d'une interception de sécurité décidée et exécutée dans le respect des dispositions légales ;
– existence d'une interception de sécurité autorisée en violation de la loi ;
– existence d'une interception « sauvage », pratiquée en violation de l'article premier du projet de loi par une personne privée ;
– absence de toute interception.

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

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

Pour être complet signalons que :
1) la Commission d'accès aux documents administratifs (CADA) arguant du secret-défense a émis le 18 décembre 1998 un avis défavorable à la demande de communication d'une copie d'une autorisation du Premier ministre concernant l'interception des communications téléphoniques d'un requérant ;
2) le Conseil d'État dans un arrêt du 28 juillet 1999 a rejeté le recours d'un requérant contre la décision du président de la CNCIS refusant de procéder à une enquête aux fins, non de vérifier si des lignes identifiées avaient fait l'objet d'une interception comme la loi lui en donne le pouvoir mais si la surveillance policière dont l'intéressé se disait victime trouvait sa source dans l'interception de lignes de ses relations.

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

Au cours de l'année 2007, la CNCIS n'a pas eu à user des dispositions du 2e alinéa de l'article 17 de la loi du 10 juillet 1991 qui précisent que *« conformément au deuxième alinéa de l'article 40 du Code de procédure pénale, la Commission donne avis sans délai au procureur de la République de toute infraction aux dispositions de la présente loi dont elle a pu avoir connaissance à l'occasion du contrôle effectué en application de l'article 15 »*.

Le contrôle du matériel

L'année 2007 a permis de prendre la mesure du changement d'économie juridique du « contrôle du matériel » (*cf.* rapport 2005, p. 31). Ce nouveau régime, issu de l'arrêté du 29 juillet 2004, participe d'une évolution de l'appréhension de ce secteur d'activité sensible par la puissance publique (*cf.* rapport 2004, p. 34 à 38 ; rapport 2005, p. 31 à 33).

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

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

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

La Commission consultative prévue à l'article R. 226-2 du Code pénal s'est réunie six fois en 2007. Sa composition est la suivante :
– le secrétaire général de la défense nationale ou son représentant, président ;
– un représentant du ministre de la Justice ;
– un représentant du ministre de l'Intérieur ;
– un représentant du ministre de la Défense ;
– un représentant du ministre chargé des douanes ;
– un représentant de la Commission nationale de contrôle des interceptions de sécurité ;
– un représentant de l'Agence nationale des fréquences ;
– deux personnalités désignées en raison de leur compétence par le Premier ministre.

La Commission a rendu, en 2007, 478 décisions ventilées comme suit :
– 302 décisions d'autorisation initiale ;

– 79 décisions de renouvellement d'autorisation ;
– 19 décisions d'ajournement ;
– 4 décisions de refus ou de retrait ;
– 74 décisions de mise « hors champ » de l'examen pour autorisation.

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

Parmi ces équipements, citons les enregistreurs qui ont représenté 40 des 74 cas de mise « hors champ » et les appareils de test et de mesure pour 27 de ce même total de 74 décisions (soit pour ces deux types de matériels 67 décisions sur les 74 considérées).

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

Chapitre III

Le contrôle des opérations de communication des données techniques (loi nº 2006-64 du 23 janvier 2006)

La loi nº 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant diverses dispositions relatives la sécurité et aux contrôles frontaliers a ouvert un nouveau chapitre dans l'activité de la Commission nationale de contrôle des interceptions de sécurité.

Cette loi, présentée au Parlement comme devant relever, dans un contexte marqué par l'hyper terrorisme, le niveau de sécurité préventive du pays en utilisant les nouvelles possibilités offertes par la technologie ou en trouvant des parades à ces mêmes moyens lorsqu'ils sont utilisés par des groupes terroristes, participe d'une évolution de la réflexion des services de police, notamment ceux chargés de la lutte contre le terrorisme, qui considèrent depuis quelques années, qu'en matière de surveillance préventive des agissements de ceux qui mettent en péril la sécurité des citoyens et des institutions démocratiques, l'accès au « contenant » est souvent plus important que l'analyse du « contenu » des communications. Autrement dit, l'écoute de la teneur des conversations des individus suspectés de terrorisme, lesquels sont par définition méfiants et prudents lorsqu'ils communiquent entre eux est moins intéressante d'un point de vue opérationnel que le recueil des « données techniques » de ces communications, lesquelles permettent d'identifier par exemple l'abonné d'un numéro repéré, d'appréhender l'environnement relationnel

d'un individu suspect (trafic de communications, facturation détaillée), voire même de retracer ou repérer ses déplacements physiques grâce notamment à la couverture des balises ou relais constituant les réseaux de communications.

Certes fort intéressante comme outil de prévention du terrorisme, cette nouvelle approche n'est pas moins potentiellement intrusive au regard de la vie privée des citoyens.

À la faveur de l'article 6 de la loi du 23 janvier 2006, le législateur, pour l'unique **prévention du terrorisme**, a donc :

• d'une part, autorisé les « agents individuellement désignés et dûment habilités » des services compétents à exiger des opérateurs de téléphonie ainsi que des fournisseurs d'accès et d'hébergement pour Internet, certaines « données techniques » relatives à une personne suspectée de menées terroristes ;

• d'autre part, confié à la Commission nationale de contrôle des interceptions de sécurité une double responsabilité :
– la nomination d'une « personnalité qualifiée » ainsi que de ses adjoints placés auprès du ministre de l'Intérieur et chargés d'accepter ou de rejeter ces demandes ;
– le contrôle *a posteriori* de ces opérations et le devoir corrélatif de saisir le ministre de l'Intérieur d'une « recommandation » quand elle *« constate un manquement aux règles… ou une atteinte aux droits et libertés »*.

Cette mission nouvelle repose de fait sur un dispositif normatif qu'il convient de rappeler ici :
– article 6 de la loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, modifié par la loi 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant diverses dispositions relatives à la sécurité et aux contrôles frontaliers ;
– article L. 34-1-1 du Code des postes et des communications électroniques ;
– décret 2006-1651 du 22 décembre 2006 pris pour l'application du I de l'article 6 de la loi 2006-64 du 23 janvier 2006 susvisée ;
– arrêté du 31 mars 2006 pris pour l'application de l'article 33 de la loi 2006-64 du 23 janvier 2006 susvisée ;
– arrêté du 10 mai 2007 pris pour l'application des dispositions de l'article R. 10-20 du Code des postes et des communications électroniques.

Il est à noter que le décret d'application de l'article 6 de la loi 2004-575 du 21 juin 2004 précité et permettant l'accès aux prestations spécifiques en matière de communications *via* Internet est, au jour de la rédaction du présent rapport, en cours d'adoption.

Il est enfin à préciser que le dispositif de l'article 6 de la loi 2006-64 du 23 janvier 2006 précitée jouit d'une durée d'applicabilité limitée au 31 décembre 2008 en vertu de l'article 32 de cette même loi. Sa prorogation devra faire l'objet, courant 2008 d'un débat et d'un vote au Parlement.

Le décret d'application de la loi du 23 janvier 2006 ayant été seulement pris le 22 décembre 2006, la mise en place de « l'équipe » de la personnalité qualifiée a pu intervenir. M. François Jaspart, personnalité qualifiée au sens de l'article 6 précité a ainsi été nommé le 26 décembre 2006. Il est assisté de six adjoints nommés dans les mêmes conditions par la Commission le 21 mars et le 28 septembre 2007.

De fait, passées les opérations de finalisation technique du dispositif, la mise en œuvre effective de l'article 6 a été réalisée le **1er mai 2007**.

La Commission a élaboré sa méthodologie de contrôle dans ce nouveau domaine. Ces modalités ont été affinées en étroit contact avec la « personnalité qualifiée » en tenant compte notamment de l'évolution qualitative et quantitative des demandes des services utilisateurs.

Au terme de huit mois d'activité et conformément aux prescriptions de l'article 6 de la loi du 23 janvier 2006, la « personnalité qualifiée » a soumis son premier rapport d'activité au président de la Commission.

Ce rapport permet de dresser un premier panorama chiffré de cette activité. Ainsi au cours de ces huit mois d'activité pour 2007, la « personnalité qualifiée » et ses adjoints ont examiné 27 701 demandes. 25 982 ont été validées, 243 ont fait l'objet d'un refus (soit 0, 87 % des demandes) et 1 476 ont fait l'objet de demandes complémentaires.

De même, il y a lieu d'observer que 73 % des demandes ont concerné des prestations relatives à l'identification de titulaires de connexions.

Il convient ici de revenir sur le chiffre des demandes validées pour indiquer qu'il ne correspond pas au nombre réel de « cibles » concernées. À l'instar de ce qui a déjà été dit sur la pluralité de vecteurs généralement détenue par la cible d'une interception de sécurité, la réalité de l'article 6 est bien loin d'une cardinalité parfaite entre nombre de demandes et nombre de « cibles ». Il n'est en effet pas rare d'observer que plusieurs dizaines de demandes concernent en fait une seule personne soupçonnée de menées terroristes.

Il apparaît, au regard de ces éléments chiffrés, que la « personnalité qualifiée » s'est inspirée de l'approche de la Commission concernant les interceptions de sécurité, en privilégiant un dialogue constructif avec les services demandeurs et en sortant d'une logique binaire acceptation/refus.

Compte tenu du volume des demandes soumises chaque semaine à la Commission (800 en moyenne), celle-ci :
– a développé un outil de gestion statistique de suivi du dispositif ;
– a exercé un « contrôle gradué », modulant le seuil de son exigence quant à la motivation en fonction du caractère plus ou moins intrusif de la prestation sollicitée au regard des libertés individuelles ;
– a mis en place des réunions bimensuelles avec la personnalité qualifiée de façon à harmoniser notamment les critères d'appréciation des motivations sur le motif terrorisme, assurant de fait une unité de jurisprudence

sur ce motif tant dans le domaine des interceptions de sécurité que dans celui de l'article 6 précité. Une dizaine d'observations est ainsi faite, à chaque réunion, à la « personnalité qualifiée » qui en tient compte par la suite lors de l'examen de nouvelles demandes.
Cette méthode a permis de limiter pour l'instant, le recours à la procédure formelle de la « recommandation » au ministre de l'Intérieur prévue à l'article L. 34-1-1, cinquième alinéa du Code des postes et communications électroniques, tel que résultant de l'article 6 de la loi du 23 janvier 2006. Pour l'instant, une seule recommandation a été formulée dans un cas de manque de base légale : le motif retenu à l'encontre de la personne faisant l'objet d'investigations sur ces « facturations détaillées », était en effet qu'elle avait spontanément dénoncé aux services de police être en possession *« d'informations sur des menaces d'attentats imminents »* …
Sauf à admettre aveuglément le principe « qui se ressemble s'assemble » lequel relève d'une sagesse populaire méfiante mais n'a pas sa place en droit, on ne peut admettre une telle motivation en contradiction avec la présomption d'innocence. On reconnaîtra cependant volontiers que sur plus de 25 000 demandes dont parfois près de cent sur la même cible, cette unique recommandation montre bien que le dialogue permanent avec la « personnalité qualifiée » a atteint son objectif ;
– a réalisé au cours de 2007 deux visites de la plateforme technique abritée par l'UCLAT et servant de support au dispositif ainsi décrit.

Deuxième partie

JURISPRUDENCE DE LA COMMISSION

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

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

La qualité de la motivation des demandes d'interception

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

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

Elle doit donc être :
– suffisante ;
– pertinente ;
– et sincère.

Une motivation suffisante

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

• En quantité :

Trois lignes ne suffisent pas. Elles ne permettent pas de cerner la personnalité de la cible, de développer un minimum les soupçons qui pèsent

sur elle, et d'expliquer la nature et la gravité du danger qu'elle fait courir à la sécurité de l'État et aux citoyens. Dans neuf cas sur dix, les « renseignements complémentaires » fournis à la demande de la Commission emporteront la conviction de cette dernière qui déplore dès lors cette regrettable insuffisance initiale d'information.

• En qualité :

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

Quelques exemples – volontairement imprécis – illustreront ces critères.

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

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

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

Une motivation pertinente

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

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

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

Une motivation sincère

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

La Commission n'a heureusement pas constaté de telles formes d'insincérité « absolue » au cours de l'année 2007.

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

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

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

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

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

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

* * *

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

Sécurité nationale

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

« Sécurité nationale », « sécurité intérieure et extérieure », « sûreté de l'État », « intérêts fondamentaux de la Nation » sont des concepts voisins souvent employés indistinctement, tout au moins pour les trois premiers. En revanche, le concept de « sécurité nationale » est apparu comme une nouveauté en 1991 et son usage est spécifique à la loi du 10 juillet 1991.

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

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

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

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

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

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

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

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

« La Commission a ainsi estimé utile de rappeler qu'il ne suffit pas d'invoquer la crainte générale d'un trouble à l'ordre public, comme y expose plus ou moins toute manifestation, pour répondre aux exigences de motivation résultant de la loi. Pour ce faire, il doit être justifié, avec la précision nécessaire, d'une menace particulièrement grave à la sécurité nationale au sens ci-dessus rappelé ».

On relève dans le même rapport (p. 36) que :
– *« la crainte d'un trouble à l'ordre public n'autorise le recours à une interception qu'en cas de menace particulièrement grave à la sécurité »* ;
– *« les interceptions de sécurité ne sauraient être utilisées comme moyen de pénétrer un milieu syndical ou politique ou de pratiquer la surveillance d'opposants étrangers, si la sécurité de l'État français lui-même n'est pas en cause »*.

La Commission est restée fidèle à cette doctrine.

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

• S'agissant de la recherche de renseignements la personne dont on se propose d'intercepter les correspondances doit être suspectée d'attenter par ses agissements personnels aux intérêts fondamentaux de la Nation. Si les services de renseignements ont, par nature, une mission de collecte de renseignements qu'ils remplissent en utilisant la palette des moyens disponibles, le recours aux interceptions de sécurité connaît

certaines limites. En effet, l'atteinte exceptionnelle à la vie privée qu'autorise la loi ne peut être justifiée même dans ce domaine que par la menace directe ou indirecte, actuelle ou future que la personne écoutée est susceptible de représenter pour la sécurité nationale. En l'absence de menace, et quel que soit l'intérêt que représente la cible comme source de renseignement pour le domaine considéré, l'atteinte à la vie privée serait contraire au principe de proportionnalité. Cette observation vaut naturellement pour les autres motifs légaux d'interception comme la prévention du terrorisme et la lutte contre la criminalité organisée même si, pour ces derniers, l'implication de la cible dans le processus conspiratif ou criminel est en principe avérée.

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

Sauvegarde du potentiel scientifique et économique de la Nation

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

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

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

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

D'autres parlementaires ont fait valoir que : « la possibilité d'interceptions de sécurité pour la protection des intérêts économiques et

scientifiques fondamentaux d'un État est reconnue par la Convention européenne des droits de l'homme, dont le texte est d'ailleurs moins restrictif que le projet de loi, puisqu'il se réfère à la notion de « bien-être économique » (*cf. supra*) ; « (…) il est nécessaire que l'État dispose de moyens d'information et d'action adaptés aux **menaces** résultant de l'internationalisation des activités économiques » (François Massot, rapport de la Commission des lois de l'Assemblée nationale, 6 juin 1991, document n° 2088, p. 29).

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

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

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

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

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

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

Le transfert illicite d'un secret de fabrication à une entité étrangère permet d'établir la réunion de plusieurs éléments constitutifs des délits de l'article 411-7 du Code pénal (on peut d'ailleurs noter que « la

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.

communication de secret de fabrique » était déjà incriminée par l'ancien article 418).

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

Il résulte de ce qui précède qu'en dépit de la définition extensive donnée au concept d'intelligence économique, les interceptions sollicitées sous le motif « sauvegarde des éléments essentiels du potentiel scientifique et économique de la France » dont la formulation est directement reprise du Code pénal et renvoie à des infractions précises, doivent d'une part répondre à une suspicion d'atteinte à ce potentiel par une menace réelle sur les recherches en cours, les brevets, le *know how* ou sur l'autonomie décisionnelle d'entreprises dont l'activité est directement liée à la sécurité ou à la défense nationale et que, d'autre part, la personne dont il est demandé d'intercepter les communications doit être personnellement impliquée dans cette menace.

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

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

Articles 2 et 3 du décret du 30 décembre 2005 :

Chapitre Ier

Dispositions relatives aux investissements étrangers en provenance de pays tiers

Article 2 – Il est inséré au chapitre III du titre V du livre Ier du même code une section 1 ainsi rédigée :

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

« Article R. 153-1 – Constitue un investissement au sens de la présente section le fait pour un investisseur :
« 1° Soit d'acquérir le contrôle, au sens de l'article L. 233-3 du Code de commerce, d'une entreprise dont le siège social est établi en France ;
« 2° Soit d'acquérir directement ou indirectement tout ou partie d'une branche d'activité d'une entreprise dont le siège social est établi en France ;
« 3° Soit de franchir le seuil de 33,33 % de détention directe ou indirecte du capital ou des droits de vote d'une entreprise dont le siège est établi en France.

« Article R. 153-2 – Relèvent d'une procédure d'autorisation au sens du I de l'article L. 151-3 les investissements étrangers mentionnés à l'article R. 153-1 réalisés par une personne physique ressortissante d'un État non membre de la Communauté européenne, par une entreprise dont le siège social se situe dans l'un de ces mêmes États ou par une personne physique de nationalité française qui y est résidente, dans les activités suivantes :
« 1° Activités dans les secteurs des jeux d'argent ;
« 2° Activités réglementées de sécurité privée ;
« 3° Activités de recherche, de développement ou de production relatives aux moyens destinés à faire face à l'utilisation illicite, dans le cadre d'activités terroristes, d'agents pathogènes ou toxiques et de prévenir les conséquences sanitaires d'une telle utilisation ;
« 4° Activités portant sur les matériels conçus pour l'interception des correspondances et la détection à distance des conversations, autorisés au titre de l'article 226-3 du Code pénal ;
« 5° Activités de services dans le cadre de centres d'évaluation agréés dans les conditions prévues au décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information ;
« 6° Activités de production de biens ou de prestation de services de sécurité dans le secteur de la sécurité des systèmes d'information d'une entreprise liée par contrat passé avec un opérateur public ou privé gérant des installations au sens des articles L. 1332-1 à L. 1332-7 du Code de la défense ;
« 7° Activités relatives aux biens et technologies à double usage énumérés à l'annexe IV du règlement (CE) n° 1334/2000 du Conseil du 22 juin 2000 modifié instituant un régime communautaire de contrôle des exportations de biens et technologies à double usage ;
« 8° Activités relatives aux moyens de cryptologie et les prestations de cryptologie mentionnés aux paragraphes III, IV de l'article 30 et I de l'article 31 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;
« 9° Activités exercées par les entreprises dépositaires de secrets de la défense nationale notamment au titre des marchés classés de défense nationale ou à clauses de sécurité conformément au décret n° 98-608 du 17 juillet 1998 relatif à la protection des secrets de la défense nationale ;

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

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

Chapitre II

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

Article 3 – Il est inséré au chapitre III du titre V du livre Ier du même code une section 2 ainsi rédigée :

« Section 2
« Dispositions relatives aux investissements en provenance des États membres de la Communauté européenne

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

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

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

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

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

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

« 2° Activités de sécurité privée, au sens de la loi nº 83-629 du 12 juillet 1983 modifiée réglementant les activités privées de sécurité, lorsque les entreprises qui les exercent :
« a) fournissent une prestation à un opérateur public ou privé d'importance vitale, au sens de l'article L. 1332-1 du Code de la défense ;
« b) ou participent directement et spécifiquement à des missions de sécurité définies aux articles L. 282-8 du Code de l'aviation civile et L. 324-5 du Code des ports maritimes ;
« c) ou interviennent dans les zones protégées ou réservées, au sens de l'article 413-7 du Code pénal et des textes pris en application du décret nº 98-608 du 17 juillet 1998 relatif à la protection des secrets de la défense nationale ;
« 3° Activités de recherche, de développement ou de production, lorsqu'elles intéressent exclusivement :
« a) les agents pathogènes, les zoonoses, les toxines et leurs éléments génétiques ainsi que leurs produits de traduction mentionnés aux alinéas 1C351 et 1C352a. 2 de l'annexe I du règlement (CE) nº 1334/2000 du Conseil du 22 juin 2000 modifié instituant un régime communautaire de contrôle des exportations de biens et technologies à double usage ;
« b) les moyens de lutte contre les agents prohibés au titre de la convention sur l'interdiction de la mise au point, de la fabrication, du stockage et de l'emploi des armes chimiques et de leur destruction, faite à Paris le 13 janvier 1993, et que le contrôle de l'investissement est exigé par les nécessités de la lutte contre le terrorisme et de la prévention des conséquences sanitaires de celui-ci ;
« 4° Activités de recherche, développement, production ou commercialisation portant sur les matériels conçus pour l'interception des correspondances et la détection à distance des conversations définis à l'article 226-3 du Code pénal, dans la mesure où le contrôle de l'investissement est exigé par les nécessités de la lutte contre le terrorisme et la criminalité ;
« 5° Activités de services dans le cadre de centres d'évaluation agréés dans les conditions prévues au décret nº 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, lorsque les entreprises qui les exercent fournissent ces prestations au profit de services de l'État, dans la mesure où le contrôle de l'investissement est exigé par les nécessités de la lutte contre le terrorisme et la criminalité ;
« 6° Activités de production de biens ou de prestations de services dans le secteur de la sécurité des systèmes d'information exercées par une entreprise liée par un contrat passé avec un opérateur public ou privé d'installation d'importance exercées par une entreprise liée par un contrat passé avec un opérateur public ou privé d'installation d'importance vitale au sens des articles L. 1332-1 à L. 1332-7 du Code de la défense pour protéger cette installation ;
« 7° Activités relatives aux biens et technologies à double usage énumérées à l'annexe IV du règlement du 22 juin 2000 précité exercées au profit d'entreprises intéressant la défense nationale. »

Prévention du terrorisme

Le terrorisme pose un problème de définition s'il n'est appréhendé que sous l'angle de l'idéologie. C'est pourquoi il est préférable de s'en tenir à une définition juridique, celle retenue, pour ce motif encore, dans le livre IV du Code pénal à l'article 421-1 qui incrimine spécialement certaines infractions quand celles-ci sont commises *« intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur »*.

Quand l'infraction commise répond aux conditions posées par cet article, il en découle d'importantes conséquences au plan de la procédure et de la répression concernant notamment les régimes de la garde à vue et des perquisitions, les règles de compétence des juridictions et de composition du tribunal, les régimes de prescription de l'action publique et de la peine, le quantum des peines principales et complémentaires encourues.

Compte tenu de l'ensemble des dispositions dérogatoires figurant notamment aux articles 421-1 et 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, pages 3795 et 3796), suppose « l'existence d'un dessein formé ou d'un plan concerté se traduisant par des efforts coordonnés en vue de l'objectif à atteindre. La notion d'entreprise exclut l'improvisation ; elle suppose des préparatifs et un minimum d'organisation (établissement d'un plan d'action, rassemblement de moyens matériels, mise en place d'un dispositif de repli, rédaction de communiqué de revendication) ».

À cet égard, un certain nombre d'actes relevant de l'expression politique violente pourraient répondre à cette définition comme l'organisation d'incidents en fin de manifestations, le démontage ou le sac symboliques de locaux publics ou privés.

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

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

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

Tout l'enjeu est là : autoriser la surveillance ciblée des individus les plus radicalisés afin de détecter à temps par exemple une dérive de type « brigadiste » sans entrer pour autant dans une police de la pensée. Caractériser une association de malfaiteurs en relation avec une entreprise terroriste en accumulant les indices sur la logistique mise en place (réseaux de financement fondés sur le don plus ou moins librement consenti, l'exploitation de commerces ne respectant pas la législation du travail, voire le crime organisé ; réseaux d'hébergement clandestin, d'infiltration ou d'exfiltration ; caches d'armes) avant que celle-ci ne soit activée pour planifier un ou plusieurs attentats qui, s'ils étaient commis, seraient mis au passif d'autorités publiques imprévoyantes ou angéliques. Autoriser la surveillance de terreaux ciblés sur lesquels la pensée terroriste peut éclore (dérive communautariste à caractère sectaire et vindicatif, endoctrinement de mineurs) sans porter atteinte à la liberté d'opinion telle que protégée par les articles 10 et 11 de la Déclaration des droits de l'homme de 1789.

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

À ce propos on notera que la préparation en France d'actes à caractère terroriste devant être commis à l'étranger 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, ou plus récemment encore l'économie souterraine.

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

Cette précision donnée, il n'est pas inutile de s'interroger sur ce concept qui, il y a peu, n'existait pas strictement à l'identique dans le Code pénal. Le Code pénal traitait quant à lui des infractions *« commises en bande organisée »*. La loi du 9 mars 2004 cependant a consacré dans le livre quatrième du Code de procédure pénale un titre vingt-cinquième à la *« procédure applicable à la 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.* rapports d'activité 1994, page 18 et 1995, page 30) et avait souligné que celle-ci résultait tant de celle retenue par la commission Schmelck, que de la définition que donne le Code pénal de la bande organisée à l'article 132-71.

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

La Commission entendait par là faciliter la lutte en amont contre la grande criminalité. L'article 132-71 du Code pénal, quant à lui, en définissant les circonstances aggravantes de certains crimes et délits, caractérise la *bande organisée* comme *« tout groupement formé ou toute entente établie en vue de la préparation, caractérisée par un ou plusieurs faits*

matériels, d'une ou plusieurs infractions ». Cette définition est également celle de l'association de malfaiteurs.

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

Depuis le 1er mars 1994, date d'entrée en vigueur du Nouveau Code pénal, la liste n'a cessé de s'allonger spécialement avec l'entrée en vigueur de la loi no 2004-204 du 9 mars 2004 dite « Perben II » qui a notamment assimilé la direction de groupement ou d'entente à caractère terroriste à une forme de criminalité organisée.

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

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

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

La bande organisée, c'est le groupement, la réunion de plusieurs malfaiteurs. Mais l'élément constitutif qui au plan pénal va permettre de distinguer la commission en bande organisée de la simple réunion, c'est, précisément, l'*organisation.* Dans la simple réunion, il n'y a ni hiérarchie ni distribution des rôles ni entente préalable en vue de commettre des infractions. La réunion est fortuite, elle est une action collective inorganisée. La commission en bande organisée suppose au contraire la préméditation. Elle suppose également un nombre de personnes supérieur à deux, chiffre qui suffit en revanche à caractériser la réunion.

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

Ainsi, la convention des Nations unies contre la criminalité transnationale organisée du 15 novembre 2000 signée par la France le 12 décembre 2003 dispose que :

a) l'expression « groupe criminel organisé » désigne un groupe structuré de trois personnes ou plus existant depuis un certain temps et agissant de concert dans le but de commettre une ou plusieurs infractions graves pour en tirer directement ou indirectement un avantage financier ou un autre avantage matériel ;

b) l'expression « infraction grave » désigne un acte constituant une infraction passible d'une peine privative de liberté dont le maximum ne doit pas être inférieur à quatre ans ou d'une peine plus lourde ;

c) l'expression « groupe structuré » désigne un groupe qui ne s'est pas constitué au hasard pour commettre immédiatement une infraction et qui n'a pas nécessairement de rôles formellement définis pour ses membres, de continuité dans sa composition ou de structure élaborée.

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

Pénalement, la circonstance de commission en bande organisée aggrave sensiblement plus les faits que la circonstance de simple réunion. Ainsi le vol en réunion est puni de 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, sous-tendus par la recherche d'un avantage financier ou matériel et menés par de véritables structures organisées composées de plus de deux acteurs, participant d'une entente préalable caractérisant une préméditation criminelle et écartant de fait la commission fortuite d'une infraction à la faveur de la circonstance aggravante de réunion.

Troisième partie

ÉTUDES ET DOCUMENTS

Chapitre I

Présentation ordonnée des textes relatifs aux missions de la Commission

Les interceptions

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

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

Les interceptions légales de correspondances émises par la voie des « communications électroniques » sont de deux types, judiciaires et de sécurité. S'agissant des interceptions judiciaires, le pluriel est employé à dessein depuis l'intervention des lois no 2002-1138 du 9 septembre 2002 et 2004-204 du 9 mars 2004.

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

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

Tableau récapitulatif des durées d'interceptions et conditions de renouvellement

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

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

Loi nº 91-646 du 10 juillet 1991 (consolidée)

TITRE I : DES INTERCEPTIONS ORDONNÉES PAR L'AUTORITÉ JUDICIAIRE

Les interceptions ordonnées en matière criminelle et correctionnelle

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

Titre III : Des juridictions d'instruction ;

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

Sous-section 2. Des interceptions de correspondances émises par la voie des télécommunications (loi nº 91-646 du 10 juillet 1991 – Titre Ier) ;

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

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

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

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

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

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

Les enregistrements sont placés sous scellés fermés. »

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

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

• Loi nº 2005-1549 du 12 décembre 2005. À peine de nullité, ne peuvent être transcrites les correspondances avec un avocat relevant de l'exercice des droits de la défense.

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

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

Article 100-7 – (*loi nº 95-125 du 8 février 1995*) – « Aucune interception ne peut avoir lieu sur la ligne d'un député ou d'un sénateur sans que le président de l'assemblée à laquelle il appartient en soit informé par le juge d'instruction.

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

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

Les interceptions ordonnées pour recherche d'une personne en fuite

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

Si les nécessités de l'enquête pour rechercher la personne en fuite l'exigent, le juge des libertés et de la détention du tribunal de grande instance peut, à la requête du procureur de la République, autoriser l'interception,

l'enregistrement et la transcription de correspondances émises par la voie des télécommunications selon les modalités prévues par les articles 100, 100-1 et 100-3 à 100-7, pour une durée maximale de deux mois renouvelable dans les mêmes conditions de forme et de durée, dans la limite de six mois en matière correctionnelle. Ces opérations sont faites sous l'autorité et le contrôle du juge des libertés et de la détention […] ».

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

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

Article 80-4 – Code de procédure pénale (loi nº 2002-1138 du 9 septembre 2002, article 66) – « Pendant le déroulement de l'information pour recherche des causes de la mort ou des causes d'une disparition mentionnée aux articles 74 et 74-1, le juge d'instruction procède conformément aux dispositions du chapitre Ier du titre III du livre Ier. Les interceptions de correspondances émises par la voie des télécommunications sont effectuées sous son autorité et son contrôle dans les conditions prévues au deuxième alinéa de l'article 100 et aux articles 100-1 à 100-7. Les interceptions ne peuvent excéder une durée de deux mois renouvelable.

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

Les interceptions ordonnées en matière de criminalité et délinquance organisées

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

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

TITRE II : DES INTERCEPTIONS DE SÉCURITÉ

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

Article 4 – *modifié par l'article 6 II de la loi no 2006-64 du 23 janvier 2006* – « L'autorisation est accordée par décision écrite et motivée du Premier ministre ou de l'une des deux personnes spécialement déléguées par lui. Elle est donnée sur proposition écrite et motivée du ministre de la Défense, du ministre de l'Intérieur ou du ministre chargé des douanes, ou *de l'une des deux personnes* que chacun d'eux aura spécialement déléguée.

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

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

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

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

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

Cette transcription est effectuée par les personnels habilités. »

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

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

Il est dressé procès-verbal de cette opération. »

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

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

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

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

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

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

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

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

Article 13 – « Il est institué une Commission nationale de contrôle des interceptions de sécurité. Cette commission est une autorité administrative indépendante. Elle est chargée de veiller au respect des dispositions

du présent titre. Elle est présidée par une personnalité désignée, pour une durée de six ans, par le Président de la République, sur une liste de quatre noms établie conjointement par le vice-président du Conseil d'État et le premier président de la Cour de cassation.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

TITRE III : DISPOSITIONS COMMUNES AUX INTERCEPTIONS JUDICIAIRES ET DE SÉCURITÉ

Article 20 – « Les mesures prises par les pouvoirs publics pour assurer, aux seules fins de défense des intérêts nationaux, la surveillance et

le contrôle des transmissions empruntant la voie hertzienne ne sont pas soumises aux dispositions des titres I et II de la présente loi. »

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

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

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

Le fait, en violation du premier alinéa, de refuser de communiquer les informations ou documents, ou de communiquer des renseignements erronés est puni de six mois d'emprisonnement et de 7500 euros d'amende. Les personnes morales peuvent être déclarées responsables pénalement dans les conditions prévues par l'article 121-2 du Code pénal de l'infraction définie au présent alinéa. Les peines encourues par les personnes morales sont l'amende, suivant les modalités prévues par l'article 131-38 du Code pénal. »

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

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

Article 226-3 – « Est puni des mêmes peines [un an d'emprisonnement et 45000 euros d'amende] la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente, en l'absence d'autorisation ministérielle dont les conditions d'octroi sont fixées par décret en Conseil

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

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

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

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

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

TITRE IV : COMMUNICATION DES DONNÉES TECHNIQUES RELATIVES À DES COMMUNICATIONS ÉLECTRONIQUES

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

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

prestataires mentionnés aux 1 et 2 du I de l'article 6 de la loi nº 2004-575 du 21 juin 2004 précitée. »

TITRE V : DISPOSITIONS FINALES

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

Textes réglementaires récents visant la loi du 10 juillet 1991

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

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

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

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

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

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

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

Article 1er – « L'obligation mise à la charge des fournisseurs de prestations de cryptologie par l'article 11-1 de la loi du 10 juillet 1991 susvisée

résulte d'une décision écrite et motivée, émanant du Premier ministre, ou de l'une des deux personnes spécialement déléguées par lui en application des dispositions de l'article 4 de la même loi.

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

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

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

Article 4 – « La décision mentionnée au premier alinéa de l'article 1er :

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

b) fixe le délai dans lequel les opérations doivent être réalisées, les modalités selon lesquelles, dès leur achèvement, le fournisseur remet aux agents visés au a) du présent article les résultats obtenus ainsi que les pièces qui lui ont été éventuellement transmises ;

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

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

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

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

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

Les opérations de communications de données techniques (loi no 2006-64 du 23 janvier 2006)

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

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

Article 6

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

« Article L. 34-1-1 – Afin de prévenir [Dispositions déclarées non conformes à la Constitution par la décision du Conseil constitutionnel no 2005-532 DC du 19 janvier 2006] les actes de terrorisme, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions peuvent exiger des opérateurs et personnes mentionnés au I de l'article L. 34-1 la communication des données conservées et traitées par ces derniers en application dudit article.

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

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

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

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

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

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

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

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

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

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

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

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

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

TITRE IV : COMMUNICATION DES DONNÉES TECHNIQUES RELATIVES À DES COMMUNICATIONS ÉLECTRONIQUES

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

Cet article appelle les commentaires suivants :

– Sur la « personnalité qualifiée » :

Les demandes relatives à ces données sont soumises à l'appréciation d'une personnalité qualifiée désignée par la Commission pour une durée de trois ans renouvelable, à partir d'une liste de trois noms proposée par le ministre de l'Intérieur. La même procédure est prévue pour la désignation des adjoints de cette personnalité. En application de l'article sus-exposé et du décret 2006-1651 du 22 décembre 2006, la Commission a désigné le 26 décembre 2006 Monsieur François Jaspart en qualité de personnalité qualifiée.

– Sur le champ d'application de cet article :

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

– Sur le contrôle des demandes :

Le texte définitivement adopté stipule que par parallélisme avec les procédures de demandes d'interceptions, que les demandes soumises à la Commission seront enregistrées, accompagnées de leur motivation et communiquées à la Commission. Le décret du 22 décembre 2006 précise

que celle-ci peut à tout moment avoir accès aux données enregistrées et demander des éclaircissements sur la motivation des demandes.

Le contrôle du matériel

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

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

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

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

Ce dispositif normatif a été enrichi par deux textes au cours de l'année 2006 :
– l'arrêté du 16 août 2006 mettant en œuvrant de manière spécifique le régime relatif au « registre » prévu par l'article R. 226-10 du Code pénal (registre retraçant la gestion des matériels soumis à autorisation). Cet arrêté a emporté l'abrogation de l'arrêté du 15 janvier 1998 qui constituait jusqu'alors le siège de cette matière ;
– l'instruction du 5 septembre 2006, véritable documentation pédagogique à l'attention des « usagers » de la réglementation relative au matériel. Elle constitue un guide pratique efficace offrant une présentation claire des modalités procédurales d'examen des demandes, ainsi que des règles de compétence de la Commission consultative dite « R. 226 ».

Ces deux textes sont reproduits ci-après.

Décrets, arrêtés, circulaires
Textes généraux
Premier ministre

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

NOR : PRMX0609553A

Le Premier ministre,
Vu le Code pénal, notamment les articles R. 226-1 et R. 226-3 et suivants ;
Vu le décret no 78-78 du 25 janvier 1978 fixant les attributions du secrétaire général de la défense nationale, notamment l'article 7-1 ;
Vu l'arrêté du 29 juillet 2004 fixant la liste d'appareils prévue par l'article R. 226-3 du Code pénal ;
Vu les arrêtés du 2 juin 2005 portant délégation de signature ;
Vu l'avis de la commission consultative chargée d'émettre un avis relatif à l'acquisition, la détention et la commercialisation des appareils susceptibles de porter atteinte à l'intimité de la vie privée ou au secret des correspondances en date du 23 mai 2006,

Arrête :

Article 1

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

Article 2

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

Article 3

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

Article 4

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

Fait à Paris, le 16 août 2006.

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

Décrets, arrêtés, circulaires
Textes généraux
Premier ministre

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

NOR : PRMX0609559J

Introduction

En vertu des articles R. 226-1 à R. 226-12 du Code pénal, le Premier ministre est compétent pour accorder les autorisations de fabrication, d'importation, d'exposition, d'offre, de location ou de vente (article R. 226-3) et d'acquisition et de détention (article R. 226-7) de matériels permettant de porter atteinte à l'intimité de la vie privée ou au secret des correspondances.

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

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

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

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

Article 1er : Instruction des demandes

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

L'article R. 226-8 du Code pénal dispose que la demande d'autorisation pour l'acquisition ou la détention de tout appareil figurant sur la liste

mentionnée à l'article R. 226-1, est déposée auprès du secrétaire général de la défense nationale (SGDN).

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

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

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

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

3° L'objet et les caractéristiques techniques du type de l'appareil, accompagnés d'une documentation technique détaillée décrivant :
– les capacités à capter, enregistrer ou transmettre, sans le consentement de leurs auteurs, des paroles prononcées à titre privé ou confidentiel ;
– les moyens éventuels de cryptologie intégrés ou intégrables dans le matériel ;
– les moyens et méthodes permettant de prévenir l'usage non autorisé du matériel ;

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

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

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

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

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

2° L'objet et les caractéristiques techniques du type de l'appareil, accompagnés d'une documentation technique détaillée décrivant :
– les capacités à capter, enregistrer ou transmettre, sans le consentement de leurs auteurs, des paroles prononcées à titre privé ou confidentiel ;
– les moyens éventuels de cryptologie intégrés ou intégrables dans le matériel ;

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

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

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

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

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

Remarques :

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

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

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

Article 2 :
Compétence de la commission consultative

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

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

La commission émet un avis sur :

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

Conformément aux termes du troisième alinéa de l'article R. 226-9, l'autorisation mentionnée à l'article R. 226-7 du Code pénal (acquisition ou détention) de tout appareil figurant en annexe de l'arrêté du 29 juillet 2004 est accordée de plein droit aux agents ou services de l'État habilités

à réaliser des interceptions autorisées par la loi, après avis de la commission consultative réunie dans son format restreint.

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

2. Les demandes d'autorisation et de renouvellement

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

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

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

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

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

2 bis. L'exposition

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

3. Les contrôles

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

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

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

4. Des arrêtés

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

Article 3 :
Conditions d'octroi des avis techniques et de moralité

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

Chaque demande est adressée par le SGDN au laboratoire technique désigné par le Premier ministre, pour avis technique. Selon le cas, un autre membre de la commission peut également être destinataire de la demande
Le laboratoire technique examine la notice technique de l'appareil objet de la demande et se rend en tant que de besoin sur place ou teste l'ensemble dans ses ateliers pour constater la conformité du matériel. Il peut saisir le ministère chargé des communications électroniques. Lorsque l'appareil comporte un émetteur radioélectrique, il saisit l'Agence nationale des fréquences avant de transmettre au SGDN un avis sans objection ou un avis défavorable motivé.
Les ministères de l'Intérieur et de la Défense adresseront un avis technique au SGDN chaque fois qu'ils le jugeront nécessaire.
Un examen de la conformité avec l'usage déclaré du matériel peut être diligenté afin de s'assurer que :
– la déclaration est conforme aux caractéristiques du matériel ;
– les fonctionnalités du matériel correspondent à l'usage déclaré.

2. Les conditions d'octroi des avis de moralité

Chaque demande est également adressée par le SGDN au ministère de la Justice, au ministère de l'Intérieur (DGPN), au ministère de la Défense (cabinet) et au ministère du Budget (direction générale des douanes). Les avis de moralité sont de la compétence :
A. – Du ministère de la Justice : son représentant fait connaître, lors de la réunion de la commission consultative, les éventuelles observations qu'appellent les différentes demandes d'autorisation présentées.
B. – De la direction générale des douanes : la direction nationale du renseignement et des enquêtes douanières fait connaître au SGDN, lors de la réunion de la commission consultative, les éventuelles observations qu'appellent les différentes demandes d'autorisation présentées.
C. – Du ministère de l'Intérieur : après enquête, la DGPN adresse au SGDN un avis sans objection ou un avis défavorable motivé dans le délai d'un mois.
D. – Du ministère de la Défense : après enquête, le ministère de la Défense adresse au SGDN un avis sans objection ou un avis défavorable motivé dans le délai d'un mois.

3. Avis des membres de la commission consultative

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

Article 4 : Retraits d'autorisation

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

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

On peut classer ces retraits en deux catégories.

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

Aux termes de l'article R. 226-11 du Code pénal, le Premier ministre, après instruction du dossier par le SGDN, peut retirer les autorisations prévues aux articles R. 226-3 et R. 226-7 dans les cas suivants :
– fausse déclaration ou faux renseignement ;
– modification des circonstances au vu desquelles l'autorisation a été délivrée ;
– lorsque le bénéficiaire de l'autorisation cesse l'exercice de l'activité pour laquelle a été délivrée l'autorisation ;
– lorsque le bénéficiaire de l'autorisation n'a pas respecté les dispositions des articles R. 226-1 à R. 226-12 ou les obligations particulières prescrites par l'autorisation.

Ainsi, constitue un motif de retrait :

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

– s'agissant des titulaires d'une autorisation de fabrication, d'importation, d'exposition, d'offre, de location ou de vente :
– le fait de ne pas tenir un registre ou de refuser de le présenter aux services enquêteurs (article R. 226-10) ;
– le fait de ne pas avoir porté, sur chaque appareil fabriqué, importé, exposé, offert, loué ou vendu, la référence du type correspondant à la demande d'autorisation (article R. 226-6) ;

– le fait d'avoir proposé, cédé, loué ou vendu des appareils à des personnes ou sociétés non autorisées (article R. 226-10) ;
– le fait de réaliser une publicité en faveur d'un appareil susceptible de permettre la réalisation des infractions prévues par l'article R. 226-1 et le second alinéa de l'article 226-15 du Code pénal lorsque cette publicité constitue une incitation à commettre ces infractions.

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

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

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

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

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

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

Chapitre II

Actualité législative et réglementaire

Article 72 de la loi nº 2007-297 du 5 mars 2007 portant création de l'article 727-1 du Code de procédure pénale

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.

Décret nº 2006-1651 du 22 décembre 2006 pris pour l'application du I de l'article 6 de la loi nº 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers

Le Premier ministre,
Sur le rapport du ministre d'État, ministre de l'Intérieur et de l'Aménagement du territoire, de la ministre de la Défense et du ministre de l'Économie, des Finances et de l'Industrie,
Vu le Code des postes et des communications électroniques, notamment ses articles L. 34-1, L. 34-1-1 et R. 10-12 à R. 10-14 ;
Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;
Vu la loi nº 91-646 du 10 juillet 1991 modifiée relative au secret des correspondances émises par la voie des communications électroniques ;
Vu la loi nº 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, notamment ses articles 6, 28, 32 et 33 ;
Vu le décret nº 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques ;
Vu l'avis de la Commission nationale de contrôle des interceptions de sécurité en date du 12 juillet 2006 ;
Vu l'avis de l'Autorité de régulation des communications électroniques et des postes en date du 7 septembre 2006 ;
Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 28 septembre 2006 ;
Vu l'avis de la Commission consultative des radiocommunications en date du 3 octobre 2006 ;
Vu l'avis de la Commission supérieure du service public des postes et des communications électroniques en date du 4 octobre 2006 ;
Vu l'avis de la Commission consultative des réseaux et services de communications électroniques en date du 11 octobre 2006 ;
Le Conseil d'État (section de l'intérieur) entendu,

Décrète :

Article 1er – Il est inséré dans la section 3 du chapitre II du titre Ier du livre II de la partie réglementaire (décrets en Conseil d'État) du Code des postes et des communications électroniques, après l'article R. 10-14, huit articles ainsi rédigés :

« Article R. 10-15. – Les agents mentionnés au premier alinéa de l'article L. 34-1-1 sont désignés par les chefs des services de police et de gendarmerie nationales chargés des missions de prévention des actes de terrorisme, dont la liste est fixée par l'arrêté prévu à l'article 33 de la loi

nº 2006-64 du 23 janvier 2006. Ils sont habilités par le directeur général ou central dont ils relèvent.

« Article R. 10-16. – Afin de permettre la désignation de la personnalité qualifiée mentionnée à l'article L. 34-1-1 et de ses adjoints, le ministre de l'Intérieur transmet à la Commission nationale de contrôle des interceptions de sécurité une liste d'au moins trois personnes, choisies en raison de leur compétence et de leur impartialité, pour chaque poste à pourvoir. Ces propositions motivées sont adressées à la commission au moins trois mois avant le terme du mandat de la personnalité qualifiée et de ses adjoints.

« La décision de la commission désignant la personnalité qualifiée et ses adjoints est notifiée au ministre de l'Intérieur et publiée au *Journal officiel de la République française*.

« Article R. 10-17. – Les demandes de communication de données prévues à l'article L. 34-1-1 comportent les informations suivantes :
a) Le nom, le prénom et la qualité du demandeur, ainsi que son service d'affectation et l'adresse de celui-ci ;
b) La nature des données dont la communication est demandée et, le cas échéant, la période concernée ;
c) La motivation de la demande.

« Article R. 10-18. – Les demandes mentionnées à l'article R. 10-17 sont transmises à la personnalité qualifiée mentionnée à l'article L. 34-1-1 par un agent désigné dans les conditions prévues à l'article R. 10-15.

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

« Article R. 10-19. – Les demandes approuvées par la personnalité qualifiée sont adressées, sans leur motivation, par un agent désigné dans les conditions prévues à l'article R. 10-15 aux opérateurs et personnes mentionnés au I de l'article L. 34-1, qui transmettent sans délai les données demandées à l'auteur de la demande.

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

« Les données fournies par les opérateurs et personnes mentionnés au I de l'article L. 34-1 sont enregistrées et conservées pendant une durée maximale de trois ans dans des traitements automatisés mis en œuvre par le ministère de l'Intérieur et le ministère de la Défense.

« Article R. 10-20. – Une copie de chaque demande est transmise, dans un délai maximal de sept jours à compter de l'approbation de la personnalité qualifiée, à la Commission nationale de contrôle des interceptions

de sécurité. Un arrêté du ministre de l'Intérieur, pris après avis de celle-ci, définit les modalités de cette transmission.

« La commission peut en outre, à tout moment, avoir accès aux données enregistrées dans les traitements automatisés mentionnés aux articles R. 10-18 et R. 10-19. Elle peut également demander des éclaircissements sur la motivation des demandes approuvées par la personnalité qualifiée.

« Article R. 10-21. – Les surcoûts identifiables et spécifiques supportés par les opérateurs et personnes mentionnés au I de l'article L. 34-1 pour la fourniture des données prévue par l'article L. 34-1-1 font l'objet d'un remboursement par l'État par référence aux tarifs et selon des modalités fixés par un arrêté conjoint du ministre de l'Intérieur et des ministres chargés du budget et des communications électroniques.

« Article R. 10-22. – Indépendamment de leur application de plein droit à Mayotte, les dispositions de la présente section sont applicables en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna. Les dispositions des articles R. 10-15 à R. 10-21 sont en outre applicables dans les Terres australes et antarctiques françaises. »

Article 2 – L'article 4 du décret du 24 mars 2006 susvisé est abrogé.

Article 3 – Le ministre d'État, ministre de l'Intérieur et de l'Aménagement du territoire, la ministre de la Défense, le ministre de l'Économie, des Finances et de l'Industrie et le ministre de l'Outre-Mer sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel de la République française*.

Fait à Paris, le 22 décembre 2006.

Par le Premier ministre : Dominique de Villepin

Décret nº 2007-1538 du 26 octobre 2007 relatif aux demandes de mise à disposition de données par voie électronique et modifiant le Code de procédure pénale (deuxième partie : décrets en Conseil d'État)

Le Premier ministre,
Sur le rapport de la garde des Sceaux, ministre de la Justice, et de la ministre de l'Intérieur, de l'Outre-Mer et des Collectivités territoriales,
Vu le Code des assurances ;
Vu le Code pénal, notamment ses articles 121-2 et 226-13 ;
Vu le Code des postes et communications électroniques, notamment son article L. 34-1 ;
Vu le Code de procédure pénale, notamment ses articles 60-2, 77-1-2 et 99-4 ;
Vu le Code rural ;
Vu le Code de la sécurité sociale ;
Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;
Vu la loi nº 2001-616 du 11 juillet 2001 relative à Mayotte ;
Vu la loi nº 2004-575 du 21 juin 2004 modifiée pour la confiance dans l'économie numérique, notamment son article 6 ;
Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 30 mai 2006
Le Conseil d'État (section de l'intérieur) entendu,

Décrète :

Article 1

I. – L'article R. 15-33-61 du Code de procédure pénale devient l'article R. 15-33-70, figurant dans une section 2 du chapitre Ier du titre II du livre Ier intitulée :

« Section 2

« Dispositions relatives aux fonctionnaires de police et militaires de la gendarmerie nationale officiers de police judiciaire ayant procédé à une déclaration d'adresse »

II. – Il est créé, au même chapitre, une section première composée des articles R. 15-33-61 à R. 15-33-69 ainsi rédigés :

« Section première

« Des demandes de mise à disposition de données par voie électronique

« Article R. 15-33-61. – Les conditions d'application des dispositions des premiers alinéas des articles 60-2, 77-1-2 et 99-4 permettant

de demander la mise à disposition de données par voie électronique au cours de l'enquête de flagrance, de l'enquête préliminaire ou de l'instruction sont fixées par les dispositions de la présente section.

« Article R. 15-33-62. – Les catégories d'organismes publics ou de personnes morales de droit privé susceptibles de faire l'objet des demandes mentionnées à l'article R. 15-33-61 sont :
1° Les opérateurs de communications électroniques tels que définis à l'article L. 34-1 du Code des postes et communications électroniques, ainsi que les personnes morales prestataires mentionnées par la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;
2° Les établissements financiers, bancaires et de crédit ;
3° Le Groupement des cartes bancaires "CB" ;
4° Les organismes sociaux mentionnés au Code de la sécurité sociale ainsi qu'au Code rural ;
5° Les entreprises d'assurance ;
6° Les organismes publics ou privés gestionnaires de logements ;
7° Les services des administrations publiques gestionnaires de fichiers administratifs, notamment fiscaux et bancaires ;
8° Les entreprises de transport collectif de voyageurs ;
9° Les opérateurs de distribution de l'énergie.

« Article R. 15-33-63. – Les demandes mentionnées à l'article R. 15-33-61 adressées aux organismes ou personnes morales relevant de l'une des catégories mentionnées à l'article R. 15-33-62 sont soumises à une procédure fixée par le protocole prévu à l'article R. 15-33-66.

« Celui-ci prévoit que les informations sollicitées par l'officier de police judiciaire sont mises à sa disposition soit dans un fichier spécifique, soit par un accès temporaire et limité à la base de données de l'organisme ou de la personne morale sollicitée.

« Article R. 15-33-64. – Peuvent seuls procéder à ces demandes les officiers de police judiciaire affectés dans un service ou une unité exerçant des missions de police judiciaire et ayant été expressément habilités à cette fin par le responsable du service ou de l'unité.

« Article R. 15-33-65. –Toute demande de mise à disposition fait l'objet de la part de l'officier de police judiciaire d'un procès-verbal indiquant le destinataire de la demande et la nature des informations demandées.

« Dans le cas prévu par l'article 77-1-2, le procès-verbal mentionne l'accord préalable du procureur de la République qui peut être donné par tout moyen.

« Article R. 15-33-66. – Les modalités techniques d'interrogation et de transmission des informations sont précisées par un protocole passé par le ministre de la Justice et, selon les cas, le ministre de l'Intérieur, le ministre de la Défense ou le ministre chargé du budget avec chaque organisme ou personne morale relevant des dispositions de l'article R. 15-33-62.

« Ce protocole précise notamment :

1° Le ou les systèmes informatiques ou traitements automatisés de données à caractère personnel intéressés ;

2° La nature des données à caractère personnel susceptibles d'être mises à disposition ;

3° Les modalités selon lesquelles l'organisme ou la personne morale permet à l'officier de police judiciaire de consulter les informations demandées et d'en effectuer vers son service le transfert par voie électronique ;

4° Les conditions et modalités de sécurisation de la liaison électronique permettant de garantir, lors de l'acheminement des informations sollicitées vers le service demandeur, l'origine, la destination, l'intégrité et la confidentialité des données ;

5° Les modalités de suivi des demandes et des consultations, incluant l'identification de l'officier de police judiciaire ;

6° Les garanties permettant de limiter la consultation aux seules informations demandées et d'empêcher tout accès à des informations protégées par un secret prévu par la loi, notamment par le secret médical, hors les cas où la loi prévoit que ce secret n'est pas opposable aux autorités judiciaires.

« Le protocole est porté à la connaissance de l'ensemble des officiers de police judiciaire des services et unités de police judiciaire ainsi que des agents des douanes relevant de l'article 28-1, qui ont été expressément habilités à procéder à ces demandes.

« Article R. 15-33-67. – Copie du protocole est adressée par l'organisme ou la personne morale à la Commission nationale de l'informatique et des libertés à l'occasion de l'accomplissement des formalités prévues par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

« Article R. 15-33-68. – L'officier de police judiciaire constate la réception des informations demandées par procès-verbal et procède soit à leur impression sur un document papier, soit à leur sauvegarde intégrale sur un support numérique conforme aux standards techniques en vigueur au moment de la transmission.

« Ce document ou ce support est annexé au procès-verbal. Si un support numérique est établi, une copie de ce support est placée sous scellés.

« Les opérations prévues à l'article R. 15-33-65 et au présent article peuvent faire l'objet d'un procès-verbal unique.

« Article R. 15-33-69. – Les données à caractère personnel recueillies en application de la présente section ne peuvent faire l'objet d'aucun traitement automatisé à l'exception de ceux nécessaires à leur exploitation dans le cadre de procédures judiciaires pénales. »

Article 2

Après l'article R. 261 du Code de procédure pénale, il est inséré un article R. 261-1 ainsi rédigé :

« Article R. 261-1. – Pour l'application de l'article R. 15-33-62, les 1° et 4° de cet article sont ainsi rédigés :
"1° Les opérateurs de communications électroniques ainsi que les personnes morales prestataires mentionnés par la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
4° Les organismes sociaux." »

Article 3

Indépendamment de son application de plein droit à Mayotte en vertu du 5° de l'article 3 de la loi nº 2001-616 du 11 juillet 2001, le présent décret est applicable dans les îles Wallis et Futuna, en Polynésie française et en Nouvelle-Calédonie.

Article 4

La ministre de l'Intérieur, de l'Outre-Mer et des Collectivités territoriales, la garde des Sceaux, ministre de la Justice, le ministre de la Défense et le ministre du Budget, des Comptes publics et de la Fonction publique sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel de la République française*.

Arrêté du 10 mai 2007 pris pour l'application des dispositions de l'article R. 10-20 du Code des postes et des communications électroniques

Le ministre de l'Intérieur et de l'Aménagement du territoire,
Vu le Code des postes et des communications électroniques, notamment ses articles L. 34-1, L. 34-1-1 et R. 10-20 ;
Vu 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, notamment son article 33 ;
Vu l'arrêté du 31 mars 2006, modifié par l'arrêté du 17 août 2006 pris pour l'application de l'article 33 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 ;
Vu l'avis de la Commission nationale de contrôle des interceptions de sécurité du 3 mai 2007,

Arrête :

Article 1 – Les demandes de communications électroniques mentionnées à l'article R. 10-17 du Code des postes et des communications électroniques sont transmises à la Commission nationale de contrôle des interceptions de sécurité (CNCIS), en application de l'article R. 10-20 du même code, sur support amovible remis à un agent de la CNCIS.

Article 2 – Le support amovible mentionné à l'article 1er dispose d'un dispositif de sécurisation par chiffrement ou, à défaut, est remis à la Commission nationale de contrôle des interceptions de sécurité sous pli scellé.

Article 3 – Le directeur général de la police nationale est chargé de l'exécution du présent arrêté, qui sera publié au *Journal officiel de la République française*.

Fait à Paris, le 10 mai 2007.

François Baroin

Chapitre III

Interceptions de sécurité et secret-défense

Aux termes de l'article 2 de **l'arrêté du 25 août 2003** relatif à la protection du secret de la défense nationale et portant instruction générale interministérielle sur la protection du secret de la défense nationale, présentent un caractère de secret de la défense nationale au sens des articles 413-9 et suivants du Code pénal les renseignements, procédés, objets, documents, données informatisées ou fichiers :
– intéressant la défense nationale qui ont fait l'objet de mesures de protection destinées à restreindre leur diffusion ;
– dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale.

Pris en application des dispositions du dernier alinéa de l'article 413-9 du Code pénal, le décret n° 98-608 du 17 juillet 1998 :
– définit trois niveaux de classification : très secret-défense, secret-défense, confidentiel-défense ;
– prévoit que les informations ou supports protégés portent la mention de leur niveau de classification.

La classification « secret-défense » d'un document ou d'une information répond, aux termes de l'article 2 de l'arrêté du 25 août 2003 susvisé, à deux exigences cumulatives :
– une exigence de fond : l'information ou le document doit intéresser la défense nationale ;
– une exigence de forme : l'apposition de la mention « secret-défense ».

La notion de défense nationale doit être entendue largement. Elle trouve sa définition dans l'article 1 de l'ordonnance 59-147 du 7 janvier 1959 portant organisation générale de la défense (ordonnance-cadre) : « La défense a pour objet d'assurer **en tout temps**, **en toutes circonstances** et **contre toutes les formes d'agression**, la sécurité et l'intégrité du territoire, ainsi que la vie de la population. »

Le rapport d'activité 2001-2003 de la Commission nationale consultative du secret de la défense nationale éclaire cette définition en ces termes : « La défense s'exerce, comme le stipule l'ordonnance de 1959 en tous temps et en tous lieux, et concerne tous les secteurs d'activité ; défense

militaire du pays, mais aussi défense civile, sécurité intérieure, protection des activités financières, économiques ou industrielles, protection du patrimoine scientifique et culturel de la France ».

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

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

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

Ainsi « Lorsque la Commission a exercé son contrôle à la suite d'une réclamation, il est notifié à l'auteur de la réclamation qu'il a été procédé aux vérifications nécessaires » (article 17 loi du 10 juillet 1991).

Chapitre IV

Jurisprudence des cours et tribunaux

L'examen des décisions rendues au sujet des interceptions de communications électroniques démontre à nouveau le caractère transversal de cette matière. Ainsi l'interception d'une communication électronique peut-elle constituer une preuve précieuse tant en droit social sur le terrain particulier du licenciement qu'en droit pénal, à condition cependant de respecter un certain nombre de conditions, que doivent régulièrement rappeler ou préciser les juridictions tant nationales qu'européennes.

En voici un aperçu pour l'année écoulée.

Jurisprudence française

Droit social et droit de la preuve

Sommaire : un employeur peut, dans certaines conditions (désignation en référé sur le fondement de l'article 145 NCPC d'un huissier qui effectue alors sa mission en présence du salarié visé) prendre connaissance des correspondances électroniques échangées par son salarié au moyen des outils professionnels mis à sa disposition.

Soc., 23 mai 2007 (05-17818)

Sur le moyen unique :

Vu l'article 145 du nouveau Code de procédure civile, ensemble les articles 9 du Code civil et L. 120-2 du Code du travail ;

Attendu que le respect de la vie personnelle du salarié ne constitue pas en lui-même un obstacle à l'application des dispositions de l'article 145 du nouveau Code de procédure civile dès lors que le juge constate que les mesures qu'il ordonne procèdent d'un motif légitime et sont nécessaires à la protection des droits de la partie qui les a sollicitées ;

Attendu, selon l'arrêt attaqué, que la société Datacep, qui employait M. X. en qualité de responsable marketing et recrutement, a obtenu du président d'un tribunal de grande instance, sur requête, une ordonnance autorisant un huissier de justice à accéder aux données contenues dans l'ordinateur mis par elle à la disposition du salarié et à prendre connaissance, pour en enregistrer la teneur, des messages électroniques échangés par l'intéressé avec deux personnes identifiées, étrangères à l'entreprise et avec lesquelles elle lui prêtait des relations constitutives, à son égard, de manœuvres déloyales tendant à la constitution d'une société concurrente ;

Attendu que pour rétracter l'ordonnance et annuler le procès-verbal dressé par l'huissier, la cour d'appel retient que la mesure d'instruction sollicitée et ordonnée a pour effet de donner à l'employeur connaissance de messages personnels émis et reçus par le salarié et en déduit qu'elle porte atteinte à une liberté fondamentale et n'est pas légalement admissible ;

Qu'en statuant ainsi, alors que l'employeur avait des motifs légitimes de suspecter des actes de concurrence déloyale et qu'il résultait de ses constatations que l'huissier avait rempli sa mission en présence du salarié, la cour d'appel a violé les textes susvisés ;

Et vu l'article 627 du nouveau Code de procédure civile ;

Par ces motifs : casse et annule dans toutes ses dispositions, l'arrêt rendu le 18 mai 2005, entre les parties, par la cour d'appel de Douai.

Sommaire : un SMS est une preuve admissible dès lors que, à la différence d'une conversation téléphonique enregistrée à l'insu de l'interlocuteur, son auteur ne peut ignorer que ce type de messages est enregistré par l'appareil récepteur.

Soc., 23 mai 2007 (06-43209) (commentaires : Recueil Dalloz, *2007, n° 23 et n° 32) ;*

Attendu, selon l'arrêt attaqué (Agen, 5 avril 2006), rendu sur renvoi après cassation (chambre sociale, 20 avril 2005, pourvoi n° Y 3 41-916), que Mme X., négociatrice immobilière à la SCP Y., Toussaint et Aragon devenue SCP Y., Aragon, Fournié, titulaire d'un office notarial, a été licenciée pour faute grave le 23 août 2000 ; qu'elle a saisi le conseil de prud'hommes en contestant son licenciement et en faisant état d'un harcèlement sexuel ;

Sur le premier moyen :

[…]

Sur le second moyen :

Attendu que la SCP notariale et M.Y. font grief à l'arrêt d'avoir déclaré établi le harcèlement sexuel de la salariée et de lui avoir alloué une somme à ce titre, alors selon le moyen :

1° que l'enregistrement et la reconstitution d'une conversation ainsi que la retranscription de messages, lorsqu'ils sont effectués à l'insu de leur auteur, constituent des procédés déloyaux rendant irrecevables en justice les preuves ainsi obtenues ; que, dès lors, en se fondant sur des messages téléphoniques d'août 1998 reconstitués et retranscrits par un huissier à l'insu de leur auteur et sur l'enregistrement d'un entretien d'avril 2000 effectué par la salariée sur une microcassette à l'insu de son employeur, la cour d'appel a violé les articles 9 du nouveau Code de procédure civile et 6 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales ;

2° qu'en imposant à M.Y. de rapporter la preuve qu'il n'était pas l'auteur des messages envoyés à partir de son téléphone portable, la cour d'appel a inversé la charge de la preuve et violé l'article 1315 du Code civil ;

3° que le juge ne peut statuer par voie de pure affirmation ; que, dès lors, en se fondant sur ce que les pressions de M.Y. s'étaient « traduites par un état dépressif de la salariée "X." qu'à compter de la mi-juin elle a été informée qu'elle n'avait plus de bureau et que le harcèlement avait eu des conséquences sur les conditions de travail de la salariée et son état de santé », sans analyser ni même préciser les pièces dont elle déduisait ces affirmations, la cour d'appel a violé l'article 455 du nouveau Code de procédure civile ;

Mais attendu que si l'enregistrement d'une conversation téléphonique privée, effectué à l'insu de l'auteur des propos invoqués, est un procédé déloyal rendant irrecevable en justice la preuve ainsi obtenue, il n'en est pas de même de l'utilisation par le destinataire des messages écrits téléphoniquement adressés, dits SMS, dont l'auteur ne peut ignorer qu'ils sont enregistrés par l'appareil récepteur ;

Et attendu qu'abstraction faite du motif surabondant tiré de l'enregistrement d'une conversation téléphonique ultérieure, la cour d'appel a constaté, par une appréciation souveraine, que les messages écrits adressés téléphoniquement à la salariée le 24 août 1998 et les autres éléments de preuve soumis à son examen établissaient l'existence d'un harcèlement ;

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

Par ces motifs : rejette le pourvoi.

Rejette le pourvoi.

Droit pénal et procédure pénale

Sommaire : la méconnaissance des formalités substantielles prévues à l'alinéa 3 de l'article 706-95 du Code de procédure pénale (information du juge des libertés et de la détention à l'issue d'une écoute ordonnée dans le cadre d'une enquête menée par le seul procureur de la République) n'entraîne pas nécessairement grief dès lors qu'un juge du siège a été mis en mesure de contrôler la régularité d'opérations attentatoires à la liberté individuelle (en l'espèce un juge d'instruction saisi par le procureur à l'issue de l'écoute).

Crim., 26 juin 2007 (07-82401)

Sur le moyen unique de cassation, pris de la violation de l'article 8 de la Convention européenne des droits de l'homme, de l'article 66 de la Constitution, des articles 171, 593, 706-95 et 802 du Code de procédure pénale, ensemble violation des droits de la défense :

en ce que la chambre de l'instruction a dit n'y avoir lieu à annuler les opérations d'interception, d'enregistrement et de transcription que le juge des libertés et de la détention a autorisées mais sur lesquelles il n'a pu exercer le contrôle prévu par l'article 706-95, alinéa 3, du Code de procédure pénale ;

Aux motifs qu'il ressort de la procédure que le juge des libertés et de la détention n'a pas été informé du déroulement des opérations d'interception contrairement aux prescriptions de l'article 706-95 du Code de procédure pénale, qui énoncent que les opérations d'interception, d'enregistrement et de transcription de correspondances prévues par les articles 100-3 à 100-5 du même code sont faites sous le contrôle du juge des libertés et de la détention, celui-ci étant informé sans délai par le procureur de la République des actes accomplis ;
que, si, comme le relève le ministère public, les prescriptions du troisième alinéa de l'article 706-95 du Code de procédure pénale ne sont pas prévues à peine de nullité, elles ont, cependant, pour objet de permettre à un juge du siège de contrôler la régularité d'opérations attentatoires à la liberté individuelle ordonnées lors d'une enquête conduite sous l'autorité du procureur de la République ; qu'il importe, dès lors, d'examiner si, en l'espèce, l'absence d'information du juge des libertés et de la détention a pu porter atteinte aux droits des parties, ainsi que le soutient l'avocat du demandeur ; que, d'une part, l'examen du dossier permet de constater que l'interception de la ligne téléphonique n° 06 14 13 96 28 a débuté, le jour fixé, le 2 février 2006, à 9 heures, pour prendre fin, avant l'expiration du délai de quinze jours prescrit, soit le 13 février 2006 ; que cette mesure a permis d'intercepter exclusivement les conversations en relation avec les faits recherchés ; qu'il apparaît que ces opérations se sont déroulées régulièrement, ce que ne conteste pas l'avocat du demandeur ; que, d'autre part, dès la fin de la mesure ordonnée, une information judiciaire a été ouverte le 1er mars 2006 et le juge d'instruction saisi a, le 7 mars suivant, ordonné la poursuite de cette interception pour une durée d'un mois ; qu'ainsi, un magistrat du siège a été informé sans délai des actes accomplis et mis en mesure d'exercer le contrôle de la régularité des opérations effectuées, notamment par la saisine de la chambre de l'instruction dans les conditions prévues par l'article 173 du Code de procédure pénale ; qu'enfin, saisie par l'avocat du mis en examen, la chambre de l'instruction est également à même de s'assurer, au vu des pièces de la procédure, du déroulement régulier de cette mesure ; qu'en conséquence, et alors que le demandeur n'a pas précisé la nature du grief qui lui aurait été causé, si ce n'est en termes abstraits, l'omission de cette prescription, pour critiquable qu'elle soit au regard des principes susmentionnés, n'a pas, en l'espèce, porté atteinte aux droits du mis en examen ;

Alors que, les dispositions de l'alinéa 3 de l'article 706-95 du Code de procédure pénale, qui prévoient que les interceptions de correspondances émises par la voie des télécommunications à l'initiative du procureur de la République sont effectuées sous le contrôle du juge des libertés et de la

détention qui les a autorisées, sont d'ordre public et dans l'intérêt d'une bonne administration de la justice ; que leur méconnaissance est constitutive d'une nullité à laquelle les dispositions de l'article 802 du Code de procédure pénale sont étrangères ; qu'en statuant comme elle l'a fait, la chambre de l'instruction a violé les textes susvisés ;

Attendu qu'il résulte de l'arrêt attaqué et des pièces de la procédure qu'au cours d'une enquête préliminaire concernant un trafic de produits stupéfiants, le procureur de la République a, sur le fondement de l'article 706-95 du Code de procédure pénale, demandé au juge des libertés et de la détention d'autoriser l'interception des communications échangées sur la ligne téléphonique utilisée par Ntangu Y. pour, selon un informateur anonyme, se livrer à la cession d'héroïne et de cocaïne ; que l'autorisation requise, donnée pour une durée de quinze jours à compter du 2 février 2006, a pris fin le 13 février ; que la procédure a été transmise le 23 février au procureur de la République qui a requis l'ouverture d'une information du chef d'infractions à la législation sur les stupéfiants, le 1er mars 2006 ;

Attendu que X., mis en examen, a excipé de la nullité des actes relatifs à cette interception téléphonique au motif que le juge des libertés et de la détention, contrairement aux prescriptions de l'article 706-95 du Code de procédure pénale, n'avait pas été informé, par le procureur de la République, des actes accomplis ;

Attendu que, pour rejeter cette requête, l'arrêt, après avoir rappelé que les prescriptions du troisième alinéa de l'article 706-95 du Code de procédure pénale ont pour objet de permettre à un juge du siège de contrôler la régularité d'opérations attentatoires à la liberté individuelle ordonnées lors d'une enquête conduite sous l'autorité du procureur de la République, énonce que les interceptions ont débuté au jour fixé par le juge, qu'elles ont pris fin avant l'expiration du délai imparti, qu'elles n'ont porté que sur les conversations en relation avec les faits recherchés et que la régularité de ces opérations n'est pas contestée par le demandeur ; que les juges ajoutent que, dès la fin de cette mesure, un juge d'instruction a été saisi et a ordonné la poursuite de cette interception en sorte qu'un magistrat du siège a été informé sans délai des actes accomplis et a pu exercer le contrôle des opérations effectuées ; qu'ils énoncent, encore, être à même de s'assurer, au vu des pièces de la procédure, du déroulement régulier de cette mesure ; qu'enfin, ils retiennent que, le demandeur n'ayant pas précisé la nature du grief qui lui aurait été causé, l'omission de la formalité prévue par la loi n'a pas, en l'espèce, porté atteinte aux intérêts du mis en examen ;

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

Qu'en effet, contrairement à ce qui est soutenu au moyen, la méconnaissance des formalités substantielles prévues par l'alinéa 3 de l'article 706-95 du Code de procédure pénale n'est constitutive d'une nullité que si l'irrégularité constatée a eu pour effet de porter atteinte aux intérêts de la partie concernée ;

Que, tel n'étant pas le cas en l'espèce, le moyen ne saurait être admis ;

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

Rejette le pourvoi.

Sommaire : l'enregistrement d'une conversation téléphonique privée est une preuve admissible au regard de l'article 6 de la CESDH, dès lors qu'elle est justifiée par la nécessité de rapporter la preuve des faits dont l'auteur est victime et par les besoins de sa défense

Crim., 31 janvier 2007 (06-82383)

Sur le moyen unique de cassation, pris de la violation des articles 427 du Code de procédure pénale, 226-1 et 441-7 du Code pénal, 6 § 1 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, défaut de motif et manque de base légale :

En ce que l'arrêt attaqué a retenu Germaine Y. dans les liens de la prévention d'usage de faux et l'a condamnée, sur l'action pénale, à quatre mois d'emprisonnement avec sursis et, sur l'action civile, à un euro de dommages-intérêts ;

Aux motifs que le procès-verbal de l'huissier a été versé au contradictoire des parties à la procédure d'instruction et la prévenue en a eu régulièrement connaissance ; que Germaine X., qui a déclaré à l'audience qu'elle savait que ses propos étaient enregistrés, ne saurait ainsi alléguer l'absence de procès équitable ; qu'il n'y a donc pas lieu d'écarter ce mode de preuve ; que le tribunal a, par des motifs pertinents que la cour adopte expressément, caractérisé l'infraction reprochée à Germaine X. ; qu'il suffit d'ajouter que la condamnation d'Arlette Z. pour l'établissement de la fausse attestation est devenue définitive, celle-ci n'en ayant pas relevé appel ; que les réponses de Germaine X. dans la conversation téléphonique enregistrée et retranscrite sur le procès-verbal de l'huissier sont très explicites sur le caractère mensonger de l'attestation et établissent la parfaite connaissance qu'avait la prévenue de la fausseté de cette pièce qu'elle a produite en justice ; que par ailleurs, les attestations établissent qu'Alain Y. était, à l'heure supposée des violences, au domicile de sa tante ; qu'il convient par conséquent de confirmer le jugement entrepris sur la culpabilité ; que le caractère de particulière gravité de la production en justice d'une fausse attestation justifie, malgré l'absence d'antécédents judiciaires de Germaine X., le prononcé d'une peine plus sévère que la cour fixe à quatre mois d'emprisonnement assorti du sursis ;

Alors que le juge ne peut fonder sa décision sur des preuves qui lui sont apportées au cours des débats par suite d'un stratagème de l'une des parties à l'encontre d'une autre ; qu'en se fondant exclusivement sur un procès-verbal d'huissier, établi à la demande d'Alain Y., retranscrivant l'enregistrement d'une conversation téléphonique avec son épouse, pour retenir cette dernière dans les liens de la prévention sans rechercher, cependant qu'elle y était dûment invitée, si cet élément de preuve n'avait pas été obtenu par suite d'un stratagème d'Alain Y., la chambre des appels correctionnels de la cour d'appel d'Aix-en-Provence a privé sa décision de toute base légale ;

Attendu qu'il résulte de l'arrêt attaqué et des pièces de procédure que Germaine X. a produit, dans une procédure de divorce, une attestation établie par une amie, relatant de graves violences commises sur elle-même par son époux, Alain Y., en état d'ébriété ; que celui-ci a porté plainte et s'est constitué partie civile des chefs d'établissement d'attestation faisant état de faits matériellement inexacts et usage et a produit un procès-verbal d'huissier retranscrivant intégralement l'enregistrement d'une conversation

téléphonique entre lui-même et son épouse, dans laquelle celle-ci reconnaissait le caractère mensonger de l'attestation ;

Attendu que, pour écarter l'argumentation de la prévenue qui invoquait le caractère déloyal de ce moyen de preuve au regard du procès équitable et la condamner du chef d'usage d'attestation inexacte, l'arrêt prononce par les motifs repris au moyen ;

Attendu qu'en statuant ainsi, et dès lors que l'enregistrement de la conversation téléphonique privée, réalisé par Alain Y., était justifié par la nécessité de rapporter la preuve des faits dont il était victime et de répondre, pour les besoins de sa défense, aux accusations de violences qui lui étaient imputées, la cour d'appel, devant qui la valeur de ce moyen de preuve a été contradictoirement débattue, n'a pas méconnu les textes et les dispositions conventionnelles visés au moyen ;

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

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

Rejette le pourvoi.

Sommaire : avant la loi n° 2004-204 du 9 mars 2004, les réquisitions tendant à obtenir d'un opérateur de téléphonie les données techniques d'appel pouvaient être établies par un officier de police judiciaire sans l'autorisation du procureur de la République. L'article 77-1-1 qui impose désormais à peine de nullité l'autorisation du procureur ne saurait s'appliquer de façon rétroactive aux réquisitions intervenues avant l'entrée en vigueur de cette loi

Crim., 20 mars 2007 (06-89250)

Attendu qu'il résulte de l'arrêt attaqué et des pièces de la procédure qu'à la suite de la plainte d'Amar Y. qui relatait avoir été enlevé et séquestré avant d'être libéré puis secouru par un de ses amis Mehena A., les fonctionnaires de police ont ouvert une enquête préliminaire ; qu'après avoir procédé à l'audition d'Amar Y. et de Mehena A., ils ont requis des opérateurs de téléphonie mobile de leur communiquer les données relatives aux appels passés et reçus avec les téléphones de ceux-ci le jour des faits ; qu'après exécution de ces réquisitions, les enquêteurs ont à nouveau entendu Mehena A. qui a reconnu avoir pris part à l'enlèvement et a donné des indications qui ont conduit à l'identification de Brahim X. ;

Attendu que ce dernier, mis en examen, a déposé une requête en annulation d'actes de la procédure faisant valoir que les réquisitions adressées aux opérateurs de téléphonie devaient être annulées, n'ayant pas été autorisées par le procureur de la République comme l'exige l'article 77-1-1 du Code de procédure pénale et que les actes qui en découlaient étaient également nuls ;

En cet état ;

Sur le premier moyen de cassation, pris de la violation des articles 6 et 8 de la Convention européenne des droits de l'homme, L. 32-3 du Code des postes et des télécommunications 60-1, 77-1-1, dans leur rédaction issue

de la loi du 18 mars 2003, 174, 591 et 593 du Code de procédure pénale, défaut de motifs, manque de base légale :

En ce que l'arrêt attaqué a rejeté la demande d'annulation des réquisitions adressées à la société SFR avant l'entrée en vigueur de la loi du 9 mars 2004 et de la procédure subséquente ;

Aux motifs qu'à juste titre le procureur général relève que les réquisitions adressées aux opérateurs de téléphonie avant la loi imposant l'autorisation préalable du parquet et la réponse apportée, quand bien même cette réponse serait postérieure à l'entrée en vigueur de cette loi, ne sont pas entachées d'irrégularité, ces dispositions étant dépourvues d'effet rétroactif ; qu'ainsi, ne sont pas entachées d'irrégularité les réquisitions, en date du 2 février 2004 (D 37), et leur résultat (D 54 à D 56) ;

Alors qu'avant l'entrée en vigueur de la loi nº 2004-204 du 9 mars 2004, aucune disposition du Code de procédure pénale ne permettait à un officier de police judiciaire, agissant dans le cadre d'une enquête préliminaire, voire en flagrance de former auprès des personnes morales de droit privé, une requête tendant à la mise à disposition d'informations utiles à la manifestation de la vérité et contenues dans un système informatique, lorsque ces informations étaient protégées par un secret prévu par la loi ; que les données relatives aux heures d'émission, destinataires et bornes d'émission de communications émises depuis un téléphone mobile sont couvertes par le secret des télécommunications ; que dès lors, la réquisition adressée à la société SFR le 2 février 2004, par un officier de police judiciaire, devait être annulée ;

Alors que subsidiairement, l'article 77-1-1 et l'article 60-1 du Code de procédure pénale, dans leur rédaction applicable à l'espèce issue de la loi du 18 mars 2003, permettaient de telles réquisitions dans le cadre de l'enquête préliminaire, lorsqu'elles ne concernaient pas des données couvertes par un secret protégé par la loi, à la condition d'avoir été autorisées par le procureur de la République ; qu'à supposer même que les informations requises auprès de la société SFR n'aient pas été couvertes par le secret des correspondances, elles ne pouvaient donc être requises qu'avec l'autorisation du procureur de la République ; que dès lors, faute d'une telle autorisation, elles devaient être annulées ;

Attendu que, pour refuser d'annuler les réquisitions adressées le 2 février 2004 et les éléments fournis en réponse, l'arrêt énonce que les dispositions de la loi du 9 mars 2004 imposant l'autorisation du procureur de la République n'ont pas d'effet rétroactif et ne peuvent concerner des réquisitions adressées avant l'entrée en vigueur de ce texte ni les réponses apportées, même si elles sont parvenues postérieurement ;

Attendu qu'en cet état et dès lors que ces réquisitions n'étaient régies ni par les dispositions de l'article 77-1-1 du Code de procédure pénale dans sa rédaction issue de la loi du 18 mars 2003, qui concernent les réquisitions intervenant par voie télématique ou informatique ni par celles du même article dans sa rédaction issue de la loi du 9 mars 2004 non encore applicables, la chambre de l'instruction a justifié sa décision ;

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

Sur le second moyen de cassation, pris de la violation des articles 6 et 8 de la Convention européenne des droits de l'homme 60-1, 77-1-1, 174, 591 et 593 du Code de procédure pénale :

En ce que l'arrêt attaqué a annulé les réquisitions adressées à la société SFR sans autorisation du procureur de la République mais a refusé d'annuler la procédure subséquente ;

[…]

D'où il suit que le moyen ne peut qu'être écarté ;

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

Rejettte le pourvoi.

Sommaire : le droit reconnu à un journaliste de ne pas révéler l'origine de ses informations n'interdit pas de retranscrire la conversation qu'il peut avoir avec une personne dont la ligne téléphonique fait l'objet d'une surveillance lorsque la mesure est nécessaire à la recherche d'une infraction et proportionnée au but à atteindre. Par ricochet, la ligne d'un journaliste peut ainsi de fait être surveillée, même si son interlocuteur est sa source.

*Crim., 30 octobre 2006 (06-85693) (*Recueil Dalloz*, 2007, n° 18)*

La Cour de cassation, Chambre criminelle, en son audience publique tenue au Palais de justice à Paris, a rendu l'arrêt suivant :

Attendu qu'il résulte de l'arrêt attaqué et des pièces de la procédure que des articles publiés, sous la signature des demandeurs, dans l'hebdomadaire Le Point *et le quotidien* L'Équipe*, ayant reproduit,* in extenso*, certains passages des procès-verbaux, non encore transmis au juge d'instruction, de transcription d'écoutes téléphoniques pratiquées pour les besoins d'une enquête sur des faits de dopage dans le milieu du cyclisme professionnel, une information a été ouverte des chefs de violation du secret de l'instruction et recel ; que les enquêteurs ont requis les opérateurs de télécommunications de leur fournir la liste des appels téléphoniques et des télécopies échangés par Dominique B., Damien C. et Étienne D., journalistes au quotidien* L'Équipe *; que des perquisitions ont été effectuées au siège des deux organes de presse ainsi qu'aux domiciles de Dominique B. et Damien C. ; qu'il a été procédé à l'interception des conversations téléphoniques d'un fonctionnaire de police qui est apparu être en relation avec Christophe X., journaliste au* Point *; que les demandeurs, mis en examen pour recel de violation du secret de l'instruction, ont présenté des requêtes en annulation d'actes de la procédure devant la chambre de l'instruction qui y a partiellement fait droit ;*

En cet état ;

[…]

Sur le second moyen de cassation, proposé pour Christophe X., Jean-Michel Y. et Olivia Z., pris de la violation de l'article 10 de la Convention européenne des droits de l'homme, 56-2, 109, 173, 175, 206, 591 et 593 du Code de procédure pénale ;

En ce que l'arrêt attaqué a dit n'y avoir lieu à annuler la pièce du dossier d'instruction cotée D. 621, relative à l'interception et à la retranscription, le 30 octobre 2004, d'une conversation téléphonique entre Christophe X. et le fonctionnaire de police Thierry E. ;

Aux motifs que la pièce D. 621 dont l'annulation est sollicitée, résulte de l'exécution de la commission rogatoire du 5 octobre 2004 ordonnant le placement sous surveillance technique de la ligne téléphonique du policier Thierry E. ; que cette mesure visait à vérifier si, parmi les policiers ayant participé à l'enquête relative au dopage au sein de l'équipe Cofidis, certains n'étaient pas susceptibles d'être les auteurs de la violation du secret de l'instruction dénoncée par le magistrat instructeur lui-même ;

Qu'ainsi, plusieurs autres policiers ont fait l'objet des mêmes mesures de surveillances techniques ; que ces mesures n'avaient pas à être accompagnées de précautions relatives au respect des sources journalistiques, même si de leurs exécutions, des conversations, comme celle interceptée entre le policier Thierry E. et le journaliste Christophe X., sont apparus ;

Qu'en conséquence, la requête en annulation formulée sur ce point sera rejetée comme mal fondée ;

Alors que, l'interception de conversations téléphoniques entre un journaliste et un policier – fût-elle le résultat de la surveillance de la ligne téléphonique de ce dernier – dans le but d'établir l'éventuelle violation par ce policier du secret de l'instruction, s'analyse en une ingérence attentatoire à la protection des sources journalistiques qui ne peut être justifiée que si elle est strictement nécessaire et proportionnée au but légitime poursuivi ;

Que dès lors, en refusant de rechercher, comme elle y était invitée, si, en l'espèce, l'interception et la retranscription le 30 octobre 2004, d'une conversation entre le journaliste Christophe X. et le policier Thierry E., ayant pour objet d'identifier ce dernier comme la source d'information du journaliste et l'auteur de la violation du secret de l'instruction poursuivie, pouvait se concilier avec les exigences de l'article 10 de la Convention européenne des droits de l'homme, au motif inopérant que cette interception avait été faite dans le cadre de la commission rogatoire plaçant sous surveillance technique la ligne téléphonique de ce policier et de plusieurs autres susceptibles d'être les auteurs de la violation du secret de l'instruction recherchée, la cour d'appel a privé sa décision de base légale au regard du texte susvisé ;

Les moyens étant réunis ;

Attendu que, pour refuser de prononcer l'annulation des perquisitions et saisies réalisées au siège du Point *et de* L'Équipe*, l'arrêt relève qu'en l'espèce, l'ingérence de l'autorité publique, au regard des droits, essentiels dans une société démocratique, à la liberté d'expression et à la protection des sources d'information des journalistes, était motivée par des faits de violation du secret de l'instruction et de recel du même délit, compromettant le déroulement de l'enquête ; que les juges ajoutent que ces perquisitions, opérées conformément aux prescriptions de l'article 56-2 du Code de procédure pénale, n'ont été décidées qu'après que des investigations longues et approfondies eurent été réalisées en vain, et qu'elles ont été effectuées rapidement dans des conditions propres à éviter une atteinte au libre exercice de la profession de journaliste et un retard injustifié à la*

diffusion de l'information ; qu'ils précisent enfin que certains des mis en examen ont déclaré avoir eu conscience des risques attachés à la publication litigieuse ;

Attendu que, pour refuser de prononcer la nullité des perquisitions réalisées aux domiciles de Dominique B. et Damien C., l'arrêt énonce, à bon droit, que les dispositions prévues par l'article 56-2 du Code de procédure pénale ne s'appliquent pas à la perquisition du domicile personnel du journaliste, qu'il soit salarié ou collaborateur occasionnel ; que les juges ajoutent qu'en l'état des investigations alors accomplies, ces actes constituaient une ingérence nécessaire et proportionnée au regard des exigences relatives au respect des sources journalistiques ;

Attendu que, pour dire n'y avoir lieu à annuler la saisie des relevés des numéros de téléphone et de télécopies utilisés par Dominique B., Damien C. et Étienne D. dans les jours précédant la parution des articles en cause, l'arrêt énonce que ces réquisitions n'ont été adressées qu'après que le juge d'instruction et les policiers eurent, en vue de découvrir les auteurs des violations du secret de l'instruction ayant permis la publication des articles de presse des 9 et 10 avril 2004, procédé à l'audition des journalistes et des fonctionnaires de police ainsi qu'à des interceptions téléphoniques visant ces derniers, toutes investigations s'étant avérées insuffisantes pour permettre la manifestation de la vérité ; que les juges relèvent encore que le caractère partiellement infructueux de ces actes d'enquête rendait nécessaire la poursuite des diligences par l'accomplissement des actes contestés ; qu'ils en concluent que les saisies et placement sous scellés ainsi opérés étaient également proportionnés au but légitime recherché ;

Attendu que, pour rejeter la demande d'annulation du procès-verbal de transcription d'une conversation téléphonique entre Christophe X. et un fonctionnaire de police dont la ligne était sous écoute, l'arrêt énonce que l'interception des conversations de ce fonctionnaire, comme celles de plusieurs autres enquêteurs, avait pour objet de vérifier si des policiers ayant participé à l'enquête relative à l'emploi de substances dopantes pouvaient avoir violé le secret de l'instruction ; qu'ils précisent que ces opérations ne sont soumises à aucune disposition particulière ;

Attendu qu'en l'état de ces motifs, desquels il résulte que l'ingérence était nécessaire et proportionnée au but légitime visé, la chambre de l'instruction a justifié sa décision au regard des exigences de l'article 10 de la Convention européenne des droits de l'homme ;

Que, d'une part, l'accomplissement d'actes d'instruction postérieurement aux perquisitions diligentées n'implique pas que ces dernières n'aient pas été indispensables au moment où elles ont été effectuées ;

Que, d'autre part, la nécessité et la proportionnalité d'un acte sont indépendantes de son résultat ;

Qu'en outre, aucune disposition n'impose de rechercher l'auteur de l'infraction de violation du secret de l'instruction avant de tenter d'identifier les auteurs d'un éventuel recel ;

Que, par ailleurs, les mesures critiquées, qui ont pour fondement des dispositions légales accessibles et prévisibles, ont été mises en œuvre en raison de la divulgation du contenu, devant légalement demeurer secret,

de pièces issues d'une information en cours et constituent des mesures justifiées tant par les impératifs d'intérêt public de protection des droits d'autrui, au nombre desquels figure la présomption d'innocence, que par la préservation d'informations confidentielles ainsi que par la nécessité de se prémunir contre des agissements de nature à entraver la manifestation de la vérité ;

Qu'enfin, le droit reconnu à un journaliste de ne pas révéler l'origine de ses informations n'interdit pas de retranscrire la conversation qu'il peut avoir avec une personne dont la ligne téléphonique fait l'objet d'une surveillance lorsque, comme en l'espèce, la mesure est nécessaire à la recherche d'une infraction et proportionnée au but à atteindre ;

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

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

Rejette les pourvois.

Jurisprudence européenne

Droit social et droit de la preuve

Sommaire : un employeur ne peut, sans risquer de violer les droits à la vie privée et au secret des correspondances protégés par l'article 6 de la CESDH, procéder à la mise sous surveillance des moyens de communication mis à la disposition de son salarié, sauf pour lui à exciper d'un texte interne autorisant et encadrant ce type d'ingérences dans la vie privée.

CEDH, 3 avril 2007, Copland contre Royaume-Uni

Résumé disponible sur le site de la CEDH : Copland – Royaume-Uni (no 62617/00)

Arrêt 3.4.2007 [Section IV]

En fait : La requérante fut engagée par un établissement d'enseignement postscolaire, un organe établi par la loi et géré par l'État, en qualité d'assistante personnelle du principal. À partir de fin 1995, elle dut travailler en étroite collaboration avec le principal adjoint. Son utilisation du téléphone, du courrier électronique et d'Internet fut surveillée à l'instigation du principal adjoint. D'après le Gouvernement, cette surveillance visait à vérifier que la requérante n'abusait pas des installations professionnelles à des fins personnelles. La surveillance de l'utilisation que l'intéressée faisait de son téléphone consista à éplucher les factures de téléphone de l'établissement d'enseignement qui indiquaient les numéros appelés, les dates et les heures des appels ainsi que la durée et le coût de ceux-ci ; la surveillance d'Internet prit la forme de vérifications des sites visités, et des heures, dates et durées de ces visites ; et le contrôle du courrier électronique consista à examiner les adresses électroniques ainsi que les dates et les heures d'envoi

des courriers. À l'époque, l'établissement d'enseignement qui employait la requérante n'avait pas de politique de surveillance. En outre, le droit anglais ne garantissait pas le droit général à la protection de la vie privée, bien que des textes de loi fussent par la suite introduits en vue de la réglementation de l'interception de communications et des conditions dans lesquelles les employeurs pouvaient enregistrer ou surveiller les communications de leurs employés sans le consentement de ceux-ci.

En droit : L'établissement d'enseignement en question est un organe public dont les actes engagent la responsabilité de l'État aux fins de la Convention. La question a donc trait à l'obligation négative de l'État de ne pas porter atteinte à la vie privée et à la correspondance de la requérante. Portée de la notion de vie privée – Les appels téléphoniques passés depuis des locaux professionnels sont de prime abord couverts par les notions de « vie privée » et de « correspondance ». Il s'ensuit logiquement que les courriers électroniques envoyés depuis le lieu de travail devraient bénéficier d'une protection analogue, tout comme le devraient les renseignements provenant de la surveillance de l'utilisation personnelle d'Internet. La requérante n'avait pas été avertie que ses appels risquaient d'être surveillés et elle pouvait donc légitimement penser que les appels passés depuis le téléphone de son lieu de travail étaient confidentiels. Elle avait probablement le même sentiment quant à son courrier électronique et à l'utilisation d'Internet. Ingérence – Le simple fait que l'établissement d'enseignement ait pu se procurer en toute légitimité les données, sous la forme de factures de téléphone, n'empêche pas de conclure à une ingérence. Peu importe également que ces renseignements n'aient pas été divulgués à des tiers ou utilisés contre la requérante dans une procédure disciplinaire ou autre. La collecte et la conservation, à l'insu de la requérante, d'informations personnelles concernant son utilisation du téléphone, du courrier électronique et d'Internet constituent par conséquent une ingérence dans l'exercice par l'intéressée de son droit au respect de sa vie privée et de sa correspondance. « Prévue par la loi » – Pour remplir l'exigence de prévisibilité, la loi doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre les mesures concernées. L'argument du Gouvernement selon lequel l'établissement concerné était autorisé, en vertu de ses prérogatives légales, à prendre « toute mesure nécessaire ou opportune » aux fins de dispenser un enseignement supérieur et postscolaire n'est pas convaincant. En outre, le Gouvernement n'avance pas qu'à l'époque des faits le droit interne général ou les textes statutaires de l'établissement d'enseignement concerné renfermaient une disposition régissant les circonstances dans lesquelles les employeurs pouvaient surveiller l'utilisation faite par les employés du téléphone, du courrier électronique et d'Internet. Par conséquent, tout en laissant ouverte la question de savoir si la surveillance de l'utilisation faite par un employé du téléphone, du courrier électronique ou d'Internet sur son lieu de travail peut passer pour « nécessaire dans une société démocratique » dans certaines situations à la poursuite d'un but légitime, la Cour conclut qu'en l'absence, à l'époque des faits, de toute loi au niveau interne régissant la surveillance, l'ingérence n'était pas « prévue par la loi ».

Conclusion : violation (unanimité). Article 41 – 3000 euros pour préjudice moral.

Droit pénal et procédure pénale

Sommaire : une condamnation pénale ne peut – sans méconnaître le droit au procès équitable protégé par l'article 8 de la CESDH – se fonder sur des interceptions de communications téléphoniques autorisées par un magistrat du ministère public sans autre garantie juridictionnelle (possibilité de contester la décision devant un organe indépendant, possibilité de vérifier le motif initial de l'interception et la qualité de la retranscription).

CEDH, 26 avril 2007, Dumitru Popescu contre Roumanie

Résumé disponible sur le site de la CEDH : Dumitru Popescu – Roumanie (no 2) (no 71525/01)

Arrêt 26.4.2007 [Section III]

En fait : Le requérant était actionnaire majoritaire d'une société d'affrètement d'avions. Soupçonné de contrebande et d'association de malfaiteurs, il fut arrêté pour son implication dans un trafic de cigarettes arrivées illégalement à l'aéroport militaire. Il fut renvoyé devant le tribunal militaire territorial. Le parquet fit parvenir à cette juridiction des transcriptions et des cassettes des écoutes téléphoniques du requérant effectuées par les services roumains de renseignement. S'appuyant notamment sur les écoutes et la liste des communications téléphoniques passées entre les inculpés, le tribunal militaire territorial déclara le requérant coupable de contrebande et association de malfaiteurs, et le condamna à douze ans d'emprisonnement. Cette condamnation fut confirmée en appel et la Cour suprême de justice rejeta le recours du requérant.

En droit : Article 8 – Seule une lecture large de la loi évoquée permettrait de considérer la disposition comme un fondement légal de l'ingérence. En matière d'interception des communications téléphoniques, il ne ressort pas clairement des pièces du dossier si une autorisation a été délivrée par le procureur pour permettre spécifiquement l'écoute des communications du requérant. Sur les garanties prévues par la loi pour assurer le degré minimal de protection voulu par la prééminence du droit dans une société démocratique, on note un manque d'indépendance des autorités compétentes pour autoriser l'ingérence.

En cas de menace pour la sûreté nationale, les communications téléphoniques pouvaient être interceptées, en vertu de la loi, par les services spéciaux de renseignements pour une durée de six mois sur simple autorisation du procureur qui pouvait la proroger pour des délais de trois mois consécutifs, sans qu'aucune limite temporelle ne soit prévue par la loi. Il s'agissait de mesures portant gravement atteinte au droit au respect de la vie privée des particuliers, et laissées à la discrétion du procureur.

Or, la Cour a déjà jugé que les procureurs roumains, agissant en qualité de magistrats du ministère public, ne remplissaient pas l'exigence d'indépendance à l'égard de l'exécutif. En outre, il existe une absence de tout contrôle a priori *des autorisations du procureur qui ne pouvaient pas être attaquées devant un organe juridictionnel indépendant et impartial, la seule voie de recours prévue par la loi contre pareilles décisions étant la contestation*

devant le procureur hiérarchiquement supérieur. Selon les dispositions nationales applicables, les personnes qui faisaient l'objet d'interceptions de leurs communications n'en étaient à aucun moment informées, et la loi ne prévoyait aucune possibilité d'introduire un recours devant un tribunal. Le contrôle a posteriori *du bien-fondé de l'interception par une autorité indépendante et impartiale était aussi inexistant. Ni les services secrets ni le procureur n'étaient obligés de verser au dossier d'instruction du tribunal saisi d'une accusation pénale, la documentation sur le fondement de laquelle ils s'étaient appuyés lorsqu'ils avaient respectivement sollicité et autorisé l'interception des communications. Or, ces lacunes de la loi semblent avoir abouti, en l'espèce, à l'impossibilité pour les tribunaux saisis de l'accusation pénale portée contre le requérant de vérifier le bien-fondé de l'autorisation donnée par le parquet ; ils se sont ainsi bornés à contrôler le respect des conditions de forme quant aux interceptions proprement dites, aux comptes rendus et aux transcriptions des communications interceptées. La simple possibilité pour un particulier prévue par la loi de saisir les commissions de la défense et de l'ordre public des deux chambres du Parlement national ne saurait suppléer à l'absence de tout contrôle* a priori *ou* a posteriori *des écoutes par une autorité judiciaire indépendante et impartiale. De plus, la loi ne prévoyait aucune sanction ou mesure que les commissions parlementaires auraient été compétentes de prendre en cas de méconnaissance de la loi par les autorités ayant réalisé ou autorisé les interceptions. Il n'y avait pas d'obligation pour le procureur de préciser dans l'autorisation les numéros de téléphone mis sur écoute, ni de garanties concernant la sauvegarde du caractère intact et complet des enregistrements et leur destruction. Le parquet a versé au dossier du tribunal des transcriptions fragmentaires des conversations téléphoniques du requérant mis sur écoute. Alors même que ceci est compréhensible dans certaines circonstances, l'intéressé doit néanmoins se voir offrir la possibilité d'écouter les enregistrements ou de contester leur véracité, d'où la nécessité de les garder intacts jusqu'à la fin du procès pénal, et de verser au dossier d'instruction les pièces qui lui semblent pertinentes pour la défense de ses intérêts. Enfin, la seule autorité nationale qui aurait pu attester la réalité et la fiabilité des enregistrements en procédant à une comparaison des voix était le service roumain de renseignements, à savoir l'autorité même qui était chargée d'intercepter les communications, de les mettre par écrit et de certifier leur authenticité. Or, dès lors qu'il y a un doute sur la réalité ou la fiabilité d'un enregistrement, il devrait y avoir une possibilité claire et effective de le faire expertiser par un centre public ou privé indépendant de celui qui a effectué les écoutes. Le Code de procédure pénale (ci-après « CPP ») comporte désormais de nombreuses garanties en matière d'interception et de transcription des communications, d'archivage des données pertinentes et de destruction de celles qui ne le sont pas. Il reste que ces changements législatifs sont largement postérieurs aux faits dénoncés par le requérant. Par ailleurs, des mesures de surveillance dans des cas d'atteinte présumée à la sûreté nationale semblent pouvoir être ordonnées aujourd'hui encore par le parquet.*

Conclusion : violation (unanimité).

Article 6 (1) – S'il est vrai que le tribunal militaire territorial statuant en première instance a refusé de renvoyer devant la Cour constitutionnelle l'exception d'inconstitutionnalité de l'article du CPP, cette omission a été réparée

en appel. Or, celle-ci a conclu à la compatibilité de la loi nationale en cause avec l'article 8 de la Convention et avec les principes qui se dégagent de la jurisprudence de la Cour en la matière. Les juridictions nationales peuvent écarter – ex officio *ou à la demande des parties – les dispositions du droit interne qu'elles jugent incompatibles avec la Convention et ses protocoles additionnels. Saisies du bien-fondé de l'accusation pénale dirigée contre le requérant, les juridictions nationales ont admis les enregistrements des communications du requérant en tant que moyen de preuve à charge, en vertu de l'article du CPP qui régissait l'utilisation des écoutes téléphoniques comme moyen de preuve au procès pénal. À cet égard, il a été loisible au requérant et à son avocat de consulter les notes du parquet contenant les transcriptions des conversations du requérant versées par le président du tribunal militaire territorial au dossier d'instruction de l'affaire. L'illégalité des écoutes téléphoniques alléguée par le requérant devant les juges nationaux se rapporte exclusivement à la méconnaissance des dispositions nationales légales de par l'absence d'autorisation du parquet le visant personnellement et de transcription intégrale des communications interceptées par les services spéciaux. Le droit procédural prévoit que les preuves n'ont pas de valeur préétablie et ne sont pas hiérarchisées, leur force probante étant fonction de l'intime conviction des juges quant à l'ensemble des preuves administrées, sans qu'il y ait donc présomption de supériorité d'une preuve sur une autre. Les enregistrements litigieux n'ont pas constitué le seul moyen de preuve soumis à l'appréciation souveraine des juges. Le tribunal militaire territorial et les juridictions supérieures ont confronté les enregistrements à d'autres éléments de preuve.*

Conclusion : non-violation (unanimité).

Article 41 – Le constat de violation de l'article 8 représente une satisfaction équitable suffisante pour le préjudice moral.

Questions parlementaires

Question écrite nº 25989 de M. Louis Souvet (Doubs – UMP)

Publiée dans le *JO* Sénat du 18 janvier 2007, page 110.

M. Louis Souvet attire l'attention de M. le ministre d'État, ministre de l'Intérieur et de l'Aménagement du territoire sur les propos tenus à l'étranger par certains acteurs politiques français n'ayant pas pu concrétiser *in fine* une démarche commerciale. C'est oublier volontairement ou involontairement que le renseignement tant géostratégique qu'économique constitue un paramètre majeur prépondérant dans ce genre de marathon mercantile, que tous les pouvoirs publics (*cf.* les alternances politiques) n'ont pas toujours contribué, loin s'en faut à la crédibilité de ces services, à leurs possibilités d'investigations. Il lui demande s'il entend renforcer les moyens dans le domaine du renseignement *via* des effectifs supplémentaires. Il rend hommage par la même occasion au travail accompli par les agents de ces différentes branches du **renseignement tant civils que militaires**, tâches ingrates puisque par essence non connues du grand public en cas de succès.

Réponse du ministère de l'Intérieur et de l'Aménagement du territoire

Publiée dans le *JO* Sénat du 12 avril 2007, page 791.

Depuis plusieurs années, la Direction de la surveillance du territoire (DST) accompagne les entreprises qui le souhaitent sur leurs marchés à l'exportation. Cette action s'inscrit exclusivement dans le cadre d'une démarche de « sécurisation économique » globale du partenaire, qu'il soit

un grand groupe, une PME-PMI ou un organisme de recherche. En effet, la **sécurité économique** est le cœur de métier de la DST service de défense comptable de la protection des intérêts nationaux. Toutefois, ce service s'interdit de faire du renseignement offensif à l'étranger car ce n'est pas son rôle. En lien permanent avec près de 4000 entreprises, laboratoires ou instituts qui travaillent principalement dans des secteurs stratégiques ou sensibles, cette direction leur apporte un soutien opérationnel et technique. Des contacts personnalisés assortis de la délivrance de conseils individualisés, des audits de sécurité, des conférences de sensibilisation qui tendent à faire prendre conscience à l'auditoire (cadres, commerciaux, responsables export notamment) des enjeux de la concurrence internationale, des conférences informatiques sur la vulnérabilité des technologies de l'information et de la communication ainsi que sur la sécurité des personnels et des informations (déstabilisation, espionnage, concurrence déloyale, désinformation) et les comportements et parades à adopter pour se protéger, sont dispensés. Ces actions concourent à la protection des stratégies commerciales, en particulier sur les marchés internationaux, des sociétés. L'efficacité de ce dispositif global d'accompagnement des entreprises repose sur la synergie des moyens dont dispose la France et qui sont restés longtemps trop dispersés. La prise en compte, ces dernières années, de l'intelligence économique, dont la sécurité économique n'est qu'une composante, en tant que politique publique permet une action efficace en la matière. Dans le cadre des créations de poste autorisées par la loi no 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure, 300 effectifs supplémentaires ont été affectés à la lutte contre le terrorisme et la criminalité organisée tant à la DST qu'à la Direction centrale des renseignements généraux (DCRG). Ainsi, la DCRG a-t-elle pu renforcer ses services consacrés à la recherche et au recueil du renseignement opérationnel par 200 fonctionnaires, dont 147 en directions régionales ou départementales. La dotation en crédits de fonctionnement et d'équipement a également été dimensionnée pour permettre à ces directions spécialisées de mettre en œuvre cet effort en matière de renseignement.

Table des matières

Sommaire 3

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 10
Financement 11

Chapitre II
Le contrôle des interceptions de sécurité (loi nº 91-646 du 10 juillet 1991) 13

Le contrôle des autorisations 13
Le contrôle de l'exécution 22
Le contrôle du matériel 26

Chapitre III
Le contrôle des opérations de communication des données techniques (loi nº 2006-64 du 23 janvier 2006) 29

Deuxième partie
JURISPRUDENCE DE LA COMMISSION 33

La qualité de la motivation des demandes d'interception 35
Sécurité nationale 38
Sauvegarde du potentiel scientifique et économique de la Nation 40
Prévention du terrorisme 46
Prévention de la criminalité et de la délinquance organisées 48

Troisième partie

ÉTUDES ET DOCUMENTS 53

Chapitre I

Présentation ordonnée des textes relatifs aux missions de la Commission 55

Les interceptions 55

Les opérations de communications de données techniques (loi nº 2006-64 du 23 janvier 2006) 68

Le contrôle du matériel 71

Chapitre II

Actualité législative et réglementaire 81

Article 72 de la loi nº 2007-297 du 5 mars 2007 portant création de l'article 727-1 du Code de procédure pénale 81

Décret nº 2006-1651 du 22 décembre 2006 pris pour l'application du I de l'article 6 de la loi nº 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers 82

Décret nº 2007-1538 du 26 octobre 2007 relatif aux demandes de mise à disposition de données par voie électronique et modifiant le Code de procédure pénale (deuxième partie : décrets en Conseil d'État) 85

Arrêté du 10 mai 2007 pris pour l'application des dispositions de l'article R. 10-20 du Code des postes et des communications électroniques 89

Chapitre III

Interceptions de sécurité et secret-défense 91

Chapitre IV

Jurisprudence des cours et tribunaux 93

Jurisprudence française 93

Jurisprudence européenne 104

Chapitre V

Questions parlementaires 109