Commission nationale de contrôle des interceptions de sécurité

35, rue Saint-Dominique
75007 Paris

Téléphone : 01 45 55 70 20
Télécopie : 01 45 55 71 15
E mail : president@commission-cncis.fr

ISBN 2-11-005412-3

Sommaire

Avant-propos 5

Première partie
RAPPORT D'ACTIVITÉ 7

Chapitre I
Organisation et fonctionnement de la Commission 9

Chapitre II
Le contrôle des autorisations 13

Chapitre III
Le contrôle de l'exécution 25

Chapitre IV
Le contrôle du matériel 31

Chapitre V
Actualités de l'année 2002 35

Chapitre VI
Avis au Premier ministre 37

Deuxième partie
ÉTUDES ET DOCUMENTS 39

Chapitre I
Présentation ordonnée des textes relatifs aux interceptions 41

Chapitre II
Textes récents relatifs aux télécommunications 53

Chapitre III
Réflexions sur le motif d'interception « prévention de la criminalité et de la délinquance organisées » 67

Chapitre IV
Réflexions sur le motif d'interceptions « prévention du terrorisme » . 73

Chapitre V
Jurisprudence européenne et française 77

Chapitre VI
Questions parlementaires 89

Chapitre VII
Les interceptions de communications en Belgique : évolutions récentes 97

Chapitre VIII
Actualités européennes 101

Avant-propos

L'année 2002 a été marquée par une activité d'interception équivalente à celle de 2001 : dans les deux cas, les chiffres traduisent, hors renouvellements d'interceptions en cours, une augmentation de 15 % sur l'année 2000. Mais la répartition dans le temps n'est pas, en 2002, ce qu'elle était en 2001 : à une progression concentrée sur la fin de l'année – après le 11 septembre – s'est substitué un flux à peu près régulier. Le début de 2003 ne paraît pas annoncer un reflux, d'autant moins que les contingents les moins élevés, ceux alloués à la gendarmerie et aux douanes, ont été augmentés sensiblement début janvier.

Les impératifs de la lutte contre le terrorisme et contre la criminalité organisée restent prédominants dans les demandes d'interception : ils en motivent près de 85 %. Les demandes des services sont examinées avec le souci de préserver le droit à la vie privée tout en faisant sa place à la protection des intérêts collectifs. Faut-il craindre que, dans une période où les risques pour la collectivité s'alourdissent, la considération prioritaire des libertés individuelles s'atténue ? Certes pas, mais, dans la pesée cas par cas qui est celle de la Commission, l'attention portée à la dangerosité s'en trouve inévitablement renforcée. Et pourtant le taux de rejet des demandes des services n'a pas diminué : il reste constant, et d'ailleurs faible. C'est sans doute parce que les services, tenus par un contingentement strict, concentrent leurs efforts sur les risques essentiels.

L'année 2002 restera, par ailleurs, une date importante pour le statut et l'organisation du groupement interministériel de contrôle (GIC). Il a, d'une part, été érigé, par le décret du 12 avril 2002, en service du Premier ministre, ce qu'il était en fait, mais non encore en droit. D'autre part, l'année a vu pratiquement s'achever la mise en place de son implantation territoriale : aux nombreux sites existants est venue se substituer une organisation reposant sur quatre régions : Île-de-France, Nord-Est, Méditerranée et Atlantique, chacune comprenant un très petit nombre d'antennes qui constituent des « GIC » déconcentrés. Ainsi se trouve assurée l'exécution de la recommandation de la CNCIS dans son rapport de 1996, tendant au « regroupement des sites en des centres bien équipés et protégés » ainsi qu'au « renforcement de l'autorité du GIC sur l'ensemble ».

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 :
Dieudonné MANDELKERN, conseiller d'État, nommé à compter du 1er octobre 1997 par le président de la République pour une durée de six ans, président,
André DULAIT, sénateur (UC) des Deux-Sèvres, désigné par le président du Sénat à la suite du renouvellement partiel du Sénat de 2001,
Henri CUQ, député (UMP) des Yvelines, désigné par le président de l'Assemblée nationale à la suite des élections législatives de juin 2002, démissionnaire, puis, à partir du 20 mars 2003, Bernard DEROSIER, député (PS) du Nord.

La Commission est assistée de deux magistrats de l'ordre judiciaire :
Gérard LORHO, délégué général depuis sa nomination en date du 17 décembre 2001,
Laurent BECUYWE, chargé de mission depuis le 3 mai 1999.

Le secrétariat est assuré par Josiane MEURICE et Françoise NUDELMANN.

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.

• *Représentants de l'Assemblée nationale*

François MASSOT, député des Alpes de Haute-Provence, 19 juillet 1991,
Bernard DEROSIER, député du Nord, 24 mai 1993,
Jean-Michel BOUCHERON, député d'Ille-et-Vilaine, 3 juillet 1997,
Henri CUQ, député des Yvelines, 4 juillet 2002,
Bernard DEROSIER, député du Nord, 20 mars 2003.

• *Représentants du Sénat*

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

• *Agents de la Commission*

– Délégués généraux

Isabelle CHAUSSADE, magistrate, 1er janvier 1993,
Mireille IMBERT-QUARETTA, magistrate, 14 juillet 1994,
Michèle SALVAT, magistrate, 19 septembre 1997,
Gérard LORHO, magistrat, 17 décembre 2001.

– Chargés de mission

Jean-Hugues GAY, magistrat, 6 septembre 1996,
Laurent BECUYWE, magistrat, 3 mai 1999.

– Secrétariat administratif

Gisèle JOUVE, 1er avril 1992,
Françoise FERBERT, 22 février 1999,
Françoise NUDELMANN, 26 février 2001.

– Secrétariat comptable

Josiane MEURICE, 21 avril 1995.

Financement

Autorité administrative indépendante, la Commission nationale de contrôle des interceptions de sécurité dispose de crédits individualisés figurant au chapitre 37-11 du budget du Premier ministre. Le président est ordonnateur des dépenses (article 18 alinéa 2 de la loi).

Pour l'année 2002, les crédits votés représentent 362 588 euros dont 267 104 au titre des frais de personnel et 95 484 au titre des frais de fonctionnement. En application de l'arrêté du 15 janvier 2003 relatif au report des crédits, la Commission a bénéficié sur son budget 2002 d'un report de 49 452 euros au titre des rémunérations, frais de personnel et prestations sociales.

Fonctionnement

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

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

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

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

Elle est représentée par ses agents aux réunions de la commission consultative créée par le décret no 97-757 du 10 juillet 1997 qui, sous la présidence du 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.

Chapitre II

Le contrôle des autorisations

Les modalités du contrôle

Déroulement du contrôle

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 pratique du contrôle préalable à la décision d'autorisation, qui a rapidement prévalu, a permis de nouer un dialogue utile avec les services demandeurs et une meilleure prise en compte par ceux-ci, en amont, des éléments de la « jurisprudence » de la Commission grâce au relais centralisé que constitue le Groupement interministériel de contrôle (GIC).

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.

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. La désignation de ces délégataires en application de l'article 4 de la loi du 10 juillet 1991 est une procédure désormais bien connue et n'appelle pas d'observation particulière.

La vérification du respect du contingent d'interception, défini par la loi comme « le nombre maximum d'interceptions susceptibles d'être pratiquées simultanément », octroyé à chacun des trois ministères autorisés à y recourir, est faite en permanence par le Groupement interministériel de contrôle et portée de manière hebdomadaire à la connaissance de la CNCIS.

Cette vérification fait ressortir en 2002 des encours moyens mensuels allant de 1 098 à 1 360 avec une moyenne annuelle, en hausse sensible, de 1 207 contre 1 108 en 2001 et 1 129 en 2000.

Si le contingent alloué en 1997 (1 540) s'est encore avéré globalement suffisant, l'extension massive du parc téléphonique imputable au GSM, notamment aux cartes prépayées, et l'impulsion donnée à la lutte contre la criminalité et la délinquance organisées, par la création des GIR (groupements d'intervention régionaux) notamment, se sont traduits au dernier trimestre 2002 par une demande d'augmentation des contingents d'interceptions au profit du ministère de la Défense et du ministère chargé des Douanes.

S'agissant du ministère de la Défense, ce sont les besoins de la gendarmerie nationale qui ont été mis en avant. Pour ce qui concerne le ministère des Finances, le quota (20), inchangé depuis 1991, n'apparaissait plus réaliste au regard de l'accroissement rapide des contrebandes diverses et des flux financiers suspects, les deux phénomènes relevant des compétences respectives de la direction générale des douanes et droits indirects (DGDDI) et du service de traitement du renseignement et action contre les circuits financiers clandestins (TRACFIN). Officiellement consultée par le Premier ministre, la Commission (*cf*. avis p. 37) a émis un avis favorable aux augmentations souhaitées qui sont applicables depuis le 1er janvier 2003. Le tableau ci-dessous résume l'évolution des contingents d'interception depuis la création de la CNCIS. La Commission avait en son temps souligné la faiblesse du contingent accordé aux Douanes et s'est montrée favorable à un relèvement du plafond.

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

Contingents	Initial 1991-1996	Modification 1997	Modification janvier 2003
Ministère de la Défense	232	330	400
Ministère de l'Intérieur	928	1 190	1 190
Ministère chargé des Douanes (DGDDI et TRACFIN)	20	20	80
Total	**1 180**	**1 540**	**1 670**

N.B. : antérieurement à la loi de 1991, les informations disponibles ne sont pas complètes. Lors du rapport de la commission Schmelck en 1982, les chiffres étaient les suivants : contingent global, 927 dont 729 pour le ministère de l'Intérieur et 198 pour la Défense. Lors de la discussion de la loi, le contingent global était de 992 provisoirement porté à 1 092 en raison de la guerre du Golfe (*source* : rapport de la commission des lois de l'Assemblée nationale, p. 15 *sq*.).

Au sein de chaque ministère existent des répartitions internes qui ne présentent pas le même caractère impératif que celui existant entre ministères. Ainsi la direction de la gendarmerie nationale, dans l'attente de l'augmentation du contingent consenti au ministère de la Défense, a-t-elle pu régulièrement dépasser son quota par prélèvement sur une autre direction du même ministère. Les contingents d'interceptions simultanées ne doivent donc pas être confondus avec le nombre total d'interceptions (demandes initiales et renouvelées) réalisés annuellement au profit des trois ministères concernés, Intérieur, Défense et Douanes. Dans son souci de conserver un caractère exceptionnel aux interceptions de sécurité, le législateur de 1991 avait opté pour une limitation sous forme d'un encours maximum. Ce système, mis en place par la décision du Premier ministre, Michel Debré, du 28 mars 1960, et résultant de pures contraintes techniques (capacité maximale d'interception et d'exploitation par le GIC) était ainsi consacré au plan des libertés publiques 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 ne peut à aucun moment dépasser un plafond fixé par ministère en vertu d'une décision du Premier ministre, puis par service par les ministres – conduit à ce que le nombre moyen annuel des interceptions est systématiquement 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.

On retrouve aux États-Unis la même notion de contingent, mais elle relève d'une autre logique : elle définit le nombre d'interceptions simultanées que tout opérateur de télécommunications doit être à même de satisfaire. Le critère de la limitation est donc celui des obligations qui peuvent être imposées aux opérateurs.

Justification de la demande d'interception de sécurité

Comme leur nom l'indique, le premier et le seul objectif des interceptions de sécurité est la sécurité des populations vivant sur notre territoire, qui fait partie des droits de l'homme dans les pays démocratiques et est une condition de la liberté. Les motifs prévus par la loi du 10 juillet 1991 ne font qu'énoncer les différents aspects de la sécurité, mais la référence précise à ceux-ci permet une première appréciation des demandes. On rappellera ici que 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 la reconstitution ou le maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées. Les services doivent faire référence à ces catégories. Ils doivent en outre justifier leur demande par des explications circonstanciées.

Le président de la CNCIS peut demander les éléments d'informations complémentaires qui lui sont nécessaires pour fonder son avis. Il exprime également les observations qu'il juge utiles sur la pertinence du motif invoqué. 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 infligée à la vie privée que constitue la surveillance de la correspondance par la voie des télécommunications, et justifier cette atteinte. Il faut encore que le but recherché ne puisse être rempli aussi bien par d'autres moyens.

Exigence de sécurité et protection des libertés

Afin d'assurer un délicat équilibre entre ces deux notions, apparemment opposées, le contrôle s'attache, d'une part, à une identification aussi précise que possible des cibles, d'autre part, aux informations recueillies sur leur activité socioprofessionnelle : il convient en effet de protéger les professions ou activités jugées sensibles en raison du rôle qu'elles jouent du point de vue des libertés fondamentales.

Il importe aussi de s'assurer que le motif légal invoqué ne dissimule pas des préoccupations autres. À cette fin sont demandés le nom et l'activité de l'abonné, le nom et la profession de l'utilisateur, et, le cas échéant, le lien qui les unit. Peuvent également être examinées en cas de doute les activités des correspondants les plus habituels ou des proches.

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'idéologies radicales, ne justifient pas en eux-mêmes une demande d'interception. De même, celles-ci ne sauraient servir à la surveillance d'opposants de pays étrangers dès lors que la sécurité de la France n'est pas menacée et que les autres objectifs mentionnés par la loi du 10 juillet 1991 ne sont pas en cause.

Données chiffrées et commentaires

Demandes initiales

Après la forte hausse constatée en 2001 (3 161 demandes contre 2 756 en 2000), les chiffres, avec un total de 3 138 demandes initiales sont restés stables et à un niveau à peu près comparable à celui des années 1998 et 1999 (respectivement 3 062 et 3 044 demandes).

Signe de cette stabilité, la moyenne mensuelle s'établit à 261 demandes contre 263 en 2001. C'est rétrospectivement 2000 qui paraît une année atypique.

Renouvellements

Avec 1 572 renouvellements, la décrue qui s'était poursuivie en 2001 (1 417 contre 1 486 en 2000) est achevée.

Comme la Commission le laissait prévoir dans son dernier rapport, la hausse importante des interceptions réalisées sur les quatre derniers mois de 2001 et consécutive aux attentats du 11 septembre s'est bien traduite par une hausse des renouvellements.

Urgences absolues

363 demandes ont été présentées selon la procédure dite d'urgence absolue, soit 11,5 % du total des demandes contre un peu plus de 12 % en 2001.

Ici encore la marque des attentats du 11 septembre est sensible ; si les demandes en urgence absolue ont baissé mensuellement par rapport aux quatre derniers mois de 2001, elles sont restées en moyenne à un niveau sensiblement supérieur à celui de l'avant-11 septembre et cette hausse est principalement imputable aux demandes présentées sous le motif « terrorisme » même si, pour le dernier trimestre – conséquence de la mise en place des GIR – les demandes présentées sous le motif « criminalité organisée » l'emportent (53 contre 35 pour la lutte contre le terrorisme).

Motifs

C'est encore la « criminalité et délinquance organisées » qui demeure le premier motif avec 1 511 demandes soit 48 %, ce qui représente encore une hausse par rapport à l'an passé (44,5 %) et légitime les augmentations de contingents d'interceptions récemment consenties. Ce motif est suivi par la lutte contre le terrorisme (35,5 %), la protection de la sécurité nationale (15,5 %) et la protection du potentiel scientifique et économique (1 %).

Les proportions sont très sensiblement différentes s'agissant des renouvellements. Le terrorisme occupe la première place avec 52 %, suivi de la sécurité nationale, 34 %, et de la délinquance organisée, 14 %.

L'explication réside dans le fait qu'en matière de criminalité organisée l'interception ne saurait se prolonger. Soit l'interception a été fructueuse et une procédure judiciaire s'en est suivie, soit elle n'a rien donné et sa prolongation ne s'est dès lors pas imposée, contrairement au long suivi que requiert la surveillance d'agents étrangers ou de réseaux suspectés de menées à caractère terroriste.

Au total (demandes initiales et renouvellements), le terrorisme représente 41 % des motifs, suivi de la criminalité organisée, 36 %, et de la sécurité nationale, 22 %. En se reportant aux premiers chiffres disponibles (rapport 1995), on relève la part quasi inchangée du terrorisme (40 %), celle légèrement supérieure de la sécurité nationale, 24 %, mais celle sensiblement plus

faible de la criminalité organisée, 29,5 %. Ce dernier motif a donc progressivement mordu sur ceux de sécurité nationale, et de protection économique.

S'agissant des demandes initiales seules, la part de la criminalité organisée qui occupait déjà la première place en 1996 avec 40 % contre 37 % pour le terrorisme a crû de 8 % en sept ans, une des étapes majeures ayant été constituée par l'augmentation du contingent du ministère de la Défense en 1997 pour satisfaire les besoins de la Gendarmerie nationale.

Bilan des observations

303 demandes (initiales et renouvellements) ont donné lieu à observations dont 104 avis négatifs (110 en 2001, 114 en 2000) :
– 53 au titre des demandes initiales, tous suivis par le Premier ministre. Ce dernier a en outre d'office opposé un refus à 3 demandes ;
– 51 au titre des demandes de renouvellements, tous suivis par le Premier ministre. Ce dernier a en outre, d'office, opposé un refus à 4 demandes. Enfin, sur demande de renseignements complémentaires, les services ont renoncé à 2 demandes.

* * *

Au total, avec 4 654 interceptions réalisées (3 082 constructions et 1 572 renouvellements) contre 4 515 en 2001, force est de constater qu'au regard du seul parc téléphonique (37,8 millions de portables et 33,9 millions de téléphones filaires) et alors que les services doivent obtenir autant d'autorisations d'interception que de numéros à intercepter pour une même personne, les interceptions de sécurité demeurent la mesure d'exception voulue par la loi. Une comparaison est possible avec les interceptions judiciaires. Pour ce faire, on ne retiendra toutefois que le chiffre des interceptions initiales de sécurité réalisées (3 082) car, s'agissant des interceptions judiciaires, les renouvellements ne sont pas comptabilisés. Pour les années 2001 et 2002, on a dénombré respectivement 9 462 et 12 711 interceptions judiciaires.

Tableaux annexes

Les demandes de construction

État des demandes initiales d'interceptions, années 2001 et 2002
Évolution mensuelle

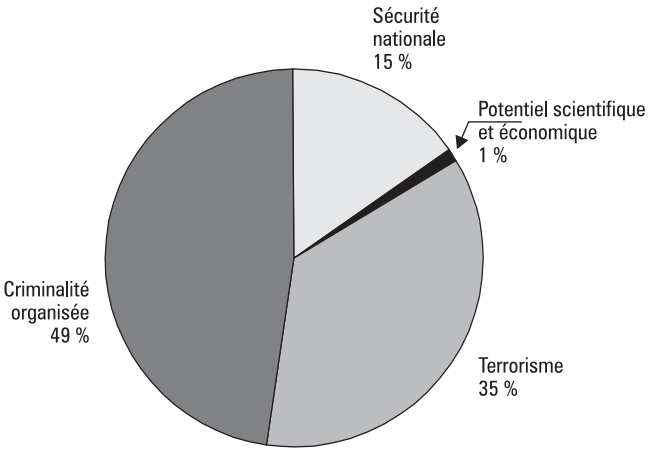
Mois	Demandes initiales de construction		Dont urgence absolue		Accordées	
	Année 2001	Année 2002	Année 2001	Année 2002	Année 2001	Année 2002
Janvier	215	225	16	30	214	219
Février	288	280	30	44	283	277
Mars	287	299	20	35	281	294
Avril	232	224	10	30	225	219
Mai	218	234	22	22	206	229
Juin	194	254	12	35	186	246
Juillet	237	302	16	26	235	300
Août	157	219	26	17	152	219
Septembre	299	215	63	28	299	213
Octobre	425	376	88	39	420	365
Novembre	313	252	47	32	306	249
Décembre	296	258	38	25	291	252
Totaux	**3 161**	**3 138**	**388**	**363**	**3 098**	**3 082**

État comparatif sur cinq ans

Motifs	1998	1999	2000	2001	2002
Sécurité nationale	491	495	449	509	486
Potentiel scientifique et économique	120	87	72	49	38
Terrorisme	1 327	1 317	979	1 203	1 103
Criminalité organisée	1 124	1 145	1 256	1 400	1 511
Groupements dissous	0	0	0	0	0
Totaux	**3 062**	**3 044**	**2 756**	**3 161**	**3 138**

Demandes initiales

Répartition des motifs



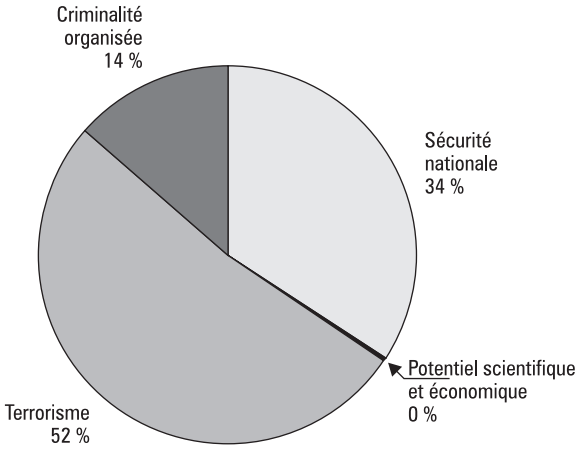
Les renouvellements d'interceptions

État mensuel des demandes des renouvellements, années 2001 et 2002

Mois	Demandes de renouvellements		Renouvellements accordés	
	Année 2001	Année 2002	Année 2001	Année 2002
Janvier	124	118	120	114
Février	99	202	93	190
Mars	170	44	166	34
Avril	83	129	76	126
Mai	180	89	178	81
Juin	111	121	108	120
Juillet	81	123	81	120
Août	162	162	158	161
Septembre	135	200	132	196
Octobre	85	115	76	115
Novembre	117	200	112	195
Décembre	117	126	117	120
Totaux	**1 464**	**1 629**	**1 417**	**1 572**

Répartition des motifs (renouvellements accordés)

Sécurité nationale	Potentiel scientifique et économique	Terrorisme	Criminalité organisée	Groupements dissous	Total
539	3	814	216	0	1 572



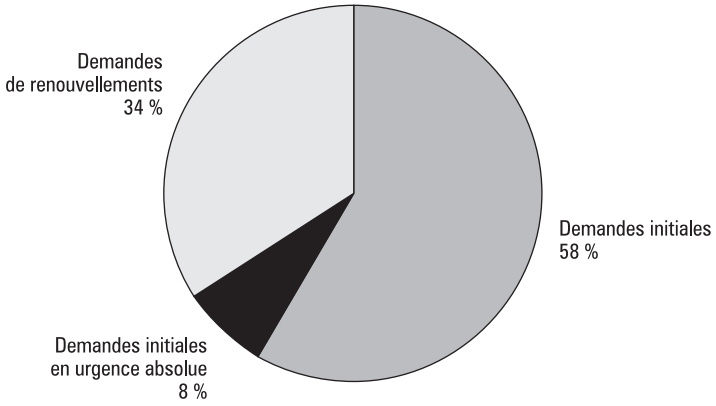
État comparatif sur cinq ans

Motifs	1998	1999	2000	2001	2002
Sécurité nationale	665	597	551	559	539
Potentiel scientifique et économique	118	99	27	17	3
Terrorisme	693	719	744	667	814
Criminalité organisée	199	181	163	174	216
Groupements dissous	9	3	1	0	0
Totaux	**1 684**	**1 599**	**1 486**	**1 417**	**1 572**

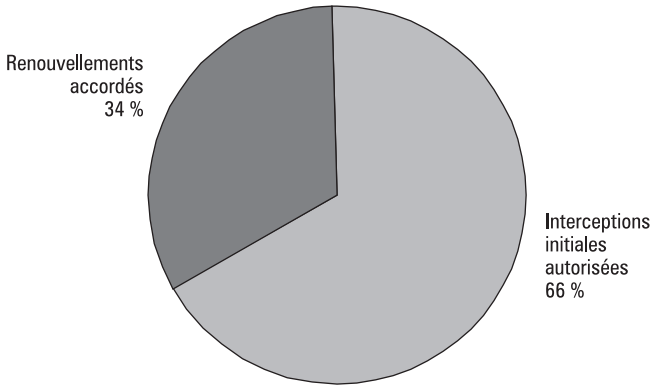
Activité de la CNCIS : demandes initiales et renouvellements

Répartition des demandes entre interceptions et renouvellements d'interceptions

Demandes initiales	Demandes initiales en urgence absolue	Demandes de renouvellements
2 775	363	1 629



Répartition entre autorisations d'interceptions et autorisations de renouvellements



Demandes d'interceptions : tableau récapitulatif global sur cinq ans

Années	Demandes initiales d'interceptions	Dont urgence absolue	Demandes de renouvellements
2002	3 138	363	1 629
2001	3 161	388	1 464
2000	2 756	197	1 533
1999	3 044	354	1 643
1998	3 062	447	1 684

Chapitre III

Le contrôle de l'exécution

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

Enregistrement, transcription et durée des interceptions

La mise en place d'une nouvelle technologie permettant l'effacement automatique 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. Le registre normalisé, mis précédemment en place pour faciliter le contrôle, a été revu pour tenir compte de cette technologie.

Lorsque la cryptologie sera davantage répandue, les contraintes du déchiffrement préalable poseront le problème des conditions d'application de ce délai.

Quant aux transcriptions, elles 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. Depuis la mise en place, en 1996, du système centralisé de contrôle des destructions pour la région parisienne, il a été observé que les transcriptions conservées par les services au-delà de quatre mois étaient devenues résiduelles.

La durée des interceptions prévue par l'article 6 de la loi du 10 juillet 1991 est de quatre mois au plus. Une interception peut toutefois être prolongée pour quatre mois par renouvellement de l'autorisation avant

l'expiration de la période en cours. La loi ne fixe pas de limite au nombre des renouvellements, mais, comme il a été dit plus haut, ceux-ci font l'objet d'une grande attention de la part de la Commission. Il va de soi que son appréciation tient compte des missions propres à chaque service.

Le contrôle du GIC

Service du Premier ministre, enfin consacré comme tel par le décret nº 2002-497 du 12 avril 2002 (voir page 50), le GIC est l'élément clé du dispositif des interceptions de sécurité. Il en assure la centralisation conformément à l'objectif posé par l'art. 4 de la loi du 10 juillet 1991 (« Le Premier ministre organise la centralisation de l'exécution des interceptions autorisées »).

Ce service est soumis à une évolution rapide, à la fois administrative et technologique, une mutation à la mesure des avancées technologiques incessantes dans le domaine des télécommunications qui constituent pour lui autant de défis à relever.

En 1996, dans son cinquième rapport d'activité, la Commission avait relevé que « si le contrôle effectif sur les opérations effectuées au GIC même ont été notablement accrues, il n'en était pas de même en ce qui concerne l'exécution assurée par les nombreux sites dispersés sur le territoire ». La Commission recommandait donc « que le regroupement des sites en des centres bien équipés et protégés, le renforcement de l'autorité du GIC sur l'ensemble doivent être accélérées en utilisant les possibilités nouvelles de centralisation que permettent les moyens informatiques ».

À la suite de cette recommandation, le GIC a entrepris, dès 1997, la mise en place de centres locaux de regroupement des interceptions, sortes de GIC déconcentrés.

Ces regroupements étaient d'ailleurs rendus inéluctables par les évolutions technologiques. À ce jour, le GIC comprend pour Paris et l'Île-de-France le centre principal des Invalides et les sites de Versailles, Bobigny et Évry. Pour la province, on recense trois zones d'exploitation : Atlantique (antennes de Bordeaux et Rennes) ; Méditerranée (antennes de Lyon et Marseille) ; Nord-Est (antennes de Lille et Nancy). Les années qui viennent devraient voir éclore des antennes secondaires qui complèteront le maillage territorial.

Les petits sites d'écoutes disséminés sur tout le territoire, souvent installés dans des conditions précaires, ni bien sécurisés, ni confortables, ont quasiment vécu.

Les représentants de la Commission qui les visitent peuvent l'attester : les antennes régionales créées disposent de locaux modernes ou réhabilités, sécurisés et bien équipés pour les agents qui y travaillent. C'est bien évidemment l'informatique, le numérique qui ont permis ces évolutions.

Déjà entre 1983 et 1986 au centre principal des Invalides, la surface des locaux consacrés à l'enregistrement, jusque-là sur bande, avait été réduite de moitié avec la « nouvelle » génération d'enregistreurs à cassettes. À partir de 1995, la numérisation des communications interceptées, leur stockage et leur exploitation informatique, parallèle à la croissance vertigineuse du GSM, ont ouvert une nouvelle voie, conduisant à la disparition rapide des cassettes.

La « cathédrale » du centre des Invalides, vaste salle ainsi nommée par ses utilisateurs en raison de sa dimension et où trônaient l'ensemble des enregistreurs à cassettes, a été désertée, l'activité, avec des capacités infiniment supérieures, étant désormais concentrée sur des surfaces considérablement réduites.

Seules les photos publiées par les journaux, faute de documents plus actuels qui seraient dans tous les cas moins spectaculaires, perpétuent le souvenir d'une époque technologiquement révolue.

Les visites sur terrain

Comme l'an passé, la CNCIS a poursuivi son action sur le terrain sous la forme de visites inopinées ou programmées des services utilisateurs d'interception, des installations et des opérateurs de télécommunication (les visites de fabricants de matériel soumis à autorisation sont évoquées dans le chapitre *ad hoc*.)

Les visites de services utilisateurs d'interceptions

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

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, quatre visites de services intéressant les régions Alsace, Aquitaine et Normandie ont été effectuées. À chaque fois, les représentants de la CNCIS dressent un inventaire des pratiques et procédures mises en œuvre par les services pour l'application de la loi du 10 juillet 1991, apportent les informations et éclaircissements utiles, notamment sur le rôle de la CNCIS, recueillent les observations des personnels rencontrés et s'informent des réalités locales se rapportant aux motifs légaux des interceptions.

Les représentants de la CNCIS se sont en outre rendus à la direction générale de la gendarmerie nationale pour y visiter la section des interceptions de sécurité. Cette structure a été créée en 1997 au sein de la DGGN afin d'assurer l'instruction et le suivi du contingent de 50 lignes qui venait d'être accordé à la Gendarmerie (*cf*. p. 14). Cette visite s'inscrivait dans l'instruction de la demande d'augmentation du contingent d'interceptions alloué au ministère de la Défense au profit de la gendarmerie. L'organisation présentée est apparue très centralisée, participant ainsi, à son niveau, à l'objectif de centralisation des interceptions voulu par la loi (art. 4). À son crédit figurent une unité de rédaction des projets d'interception soumis par les sections de recherche, une unité de l'instruction intrinsèque et extrinsèque des demandes, la sécurisation des projets d'interception et de leur suivi, la régulation de l'urgence. La centralisation, au niveau régional puis au niveau national, qui en résulte pourrait inspirer une inquiétude si elle n'était compensée par une bonne réactivité dans le circuit de l'information ascendante (validation du projet d'interception) et descendante (examen quotidien des productions et restitution éventuelle aux enquêteurs locaux). La section doit naturellement se renforcer en moyens humains et matériels pour conserver le même niveau de réactivité compte tenu de l'augmentation du contingent consenti.

Les visites des opérateurs de télécommunications

Ont été successivement visités : SFR (groupe Cegetel) le 17 avril 2002, Bouygues Telecom le 6 mai et Orange le 21 juin. Ces trois opérateurs GSM disposent sous des intitulés proches d'un service dit des obligations légales, souvent couplé en raison des impératifs de sécurité qui y sont attachés à un service de prévention des fraudes.

En raison des volumes traités, les trois opérateurs ont organisé leur service des obligations légales sous forme de plateau. Le plus fort pourcentage de leur activité, est, en effet, consacré à la satisfaction des réquisitions, essentiellement judiciaires d'identification de numéros. Les réquisitions en nombre variable par opérateur, en fonction de leur part de marché respective (de 8000 à 25000 par mois) mais toujours croissant, sont transmises par fax et traitées par au moins une dizaine de personnes couvrant de larges plages horaires avec régime d'astreinte en dehors des heures ouvrables. Une part plus restreinte de leurs obligations légales est consacrée au traitement des demandes d'interception judiciaire et de sécurité avec, ici encore, une part prépondérante (70 % environ) pour les interceptions judiciaires.

Les représentants de la CNCIS ont pu s'assurer à l'occasion de ces visites du bon niveau de sécurisation des locaux et ont vérifié le respect des conditions posées par les articles 1 et 2 du décret n° 93-119 du 28 janvier 1993 relatif à la désignation des agents qualifiés pour la réalisation des opérations matérielles nécessaires à la mise en place des interceptions de correspondance (antériorité d'emploi d'au moins deux ans chez l'opérateur ; absence de condamnation pénale inscrite au bulletin n° 2 du casier judiciaire).

Réclamations de particuliers et dénonciation à l'autorité judiciaire

Les saisines de la CNCIS par les particuliers

Cette année la CNCIS a été saisie par écrit de 34 réclamations de particuliers. Une minorité 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 nombre de requérants se sont adressés à la CNCIS téléphoniquement avant toute démarche écrite. Ce contact préalable a 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 dysfonctionnement techniques classiques ; il a également permis de réorienter les demandeurs vers les services ou autorités compétents.

Il convient de rappeler que le pouvoir d'investigation exercé sur le fondement de l'article 15 a été précisé par le Conseil d'État en un arrêt du 28 juillet 1999. Aux termes de cet arrêt, ce pouvoir ne saurait être étendu à l'origine des informations ayant déclenché une action des services de police.

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

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 ». Ce devoir de dénonciation à l'autorité judiciaire est le corollaire du pouvoir de contrôle de la Commission et signifie que, dans cette hypothèse, la Commission est exonérée du respect du secret-défense qui pèse sur la matière.

Rappelons que la disposition de l'article 17, alinéa 2 est comparable à celle énoncée dans l'article 21, 4e alinéa de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés qui prévoit que la CNIL « dénonce au parquet les infractions dont elle a connaissance conformément à l'article 40 du Code de procédure pénale ».

Ce devoir de signalement et sa portée ont été plus longuement commentés dans le rapport de l'année 2000.

Chapitre IV

Le contrôle du matériel

Le rapport de la CNCIS pour l'année 2001 a, à l'occasion du dixième anniversaire de la Commission, rappelé le processus qui avait conduit à la mise en place puis à la modification des textes réglementaires régissant les matériels d'écoute [1]. On peut s'y reporter utilement. Rappelons simplement ici le cadre juridique. Il se résume à quatre séries de textes : tout d'abord, l'article 226-3 du Code pénal qui dispose que « est punie des mêmes peines [2] 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 [3] ou qui, conçus pour la détection à distance des conversations, permettent de réaliser l'infraction prévue par l'article 226-1 [4] et figurant sur une liste dressée dans des conditions fixées par ce même décret [...] » ; ensuite, les articles R. 226-1 à -12 du même Code, qui organisent les conditions et modalités de délivrance des autorisations ; puis l'arrêté du 9 mai 1994 fixant la liste des appareils prévue à l'article 226-3, repris ci-dessus ; et enfin l'arrêté du 15 janvier 1998 relatif au registre visé par l'article R. 226-10.

1) CNCIS, 10e rapport d'activité 2001, page 25.
2) Un an d'emprisonnement et 45 000 € d'amende (*cf.* art. 226-1 CP).
3) L'atteinte au secret des correspondances émises par la voie de télécommunications.
4) L'atteinte à la vie privée par captage, enregistrement ou transmission de paroles privées ou confidentielles.

En 2002, la commission consultative compétente pour donner les avis sur les demandes d'acquisition/détention ou commercialisation des matériels visés par cette réglementation s'est réunie sept fois. 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 du ministre chargé de l'Industrie ;
– un représentant du ministre chargé des Télécommunications ;
– un représentant de la Commission nationale de contrôle des interceptions de sécurité ;
– un représentant du directeur général de l'Agence nationale des fréquences ;
– deux personnalités choisies en raison de leurs compétences, désignées par le Premier ministre.

550 dossiers ont été présentés en 2002. Concernant chacun un ou plusieurs matériels, ils ont donné lieu à la délivrance de 1 050 autorisations et 4 refus (3 concernaient des demandes d'acquisition/détention et 1 une demande de commercialisation).

On observe ici que le tassement du nombre des autorisations délivrées constaté l'année dernière non seulement se confirme mais s'amplifie puisque la variation 2001-2002 devient négative, la diminution étant de 16,4 % (1 050 contre 1 256).

La répartition du nombre de dossiers de demandes initiales et de renouvellements (respectivement 84,20 % et 15,80 % en 2002 contre 94 % et 6 % en 2001) [1] conforte l'analyse ébauchée l'année dernière selon laquelle on peut apparemment considérer que tous les acteurs du marché se sont manifestés et que l'arriéré des situations qui devaient être régularisées depuis la réforme de 1997 est entièrement épongé.

S'agissant des autorisations d'acquisition/détention initiales, elles ne devraient à l'avenir correspondre qu'à des nouveaux détenteurs et non plus à des régularisations de situations en infraction à la réglementation.

Pour les autorisations de commercialisation, il s'agira soit de nouvelles entreprises sur le marché (on en a compté 24 en 2002), soit d'entreprises déjà connues mais proposant de nouveaux matériels ou des appareils déjà autorisés mais dotés de nouvelles fonctionnalités.

À cet égard, la CNCIS regrette l'absence d'une documentation officielle facilement accessible et exposant de façon synthétique la réglementation et les autorités à saisir. Il faut se résoudre à admettre que, si ce niveau de

1) En 2002 : 550 dossiers dont 463 demandes initiales et 87 renouvellements ;
en 2001 : 633 dossiers dont 595 demandes initiales et 38 renouvellements.

conformité aux règles régissant la matière a été atteint, cela résulte principalement de la diffusion de l'information par les professionnels de la commercialisation, entre eux et vers leurs clients.

En dehors de sa participation à la commission consultative, la préoccupation de la CNCIS au sujet des matériels se concrétise également par des visites du délégué général et du chargé de mission chez les fabricants ou les revendeurs.

Ces déplacements comportent une part de veille technologique mais ils sont aussi pour la CNCIS un moyen de connaître l'état du marché. Elle a, en effet, toujours considéré qu'au-delà du suivi exhaustif des demandes d'interceptions présentées par les services, elle devait contribuer à la protection de la vie privée en participant à la lutte contre les tentatives de contournements de la loi et particulièrement les écoutes « sauvages ».

Dans cet esprit, certains services de l'État, titulaires d'autorisations de « plein droit » conformément au nouveau régime mis en place l'année dernière [1], ont été invités à produire leurs registres et à expliquer leurs règles internes de gestion des matériels sensibles. Ces rencontres ont permis aux représentants de la CNCIS de constater la bonne volonté des services et de s'assurer de l'adéquation des matériels achetés avec leurs missions.

Selon la CNCIS, et cette affirmation n'est pas nouvelle, la vraie menace d'atteinte à la vie privée vient d'individus ou officines peu scrupuleux. Il peut être, en effet, facile, étant animé de mauvaises intentions, de se procurer des appareils notamment grâce à l'internet ou grâce aux différences de régime juridique au sein de l'Union européenne et à la liberté de circulation des personnes et des biens. Sur le marché intérieur, cette situation a conduit un fabricant à saisir le secrétaire général de la défense nationale d'une demande de modification de l'arrêté de 1994 fixant la liste des matériels soumis à autorisation : alors qu'il est respectueux des règles, il voit certains clients se tourner vers d'autres sources.

L'opinion de la CNCIS, exprimée à cette occasion, est qu'il faut, non pas assouplir les textes, mais au contraire en assurer le respect et à cette fin renforcer les contrôles. Dans une matière où les risques d'atteintes à la vie privée sont réels, la rigueur s'impose ; la lucidité et la modestie également.

En effet, l'on ne peut ignorer la critique selon laquelle seules les personnes de bonne volonté (celles dont les libertés n'ont *a priori* rien à craindre) se soumettent au régime d'autorisation des matériels.

La réponse est que l'intérêt majeur de ce système est de permettre, à l'image du régime des armes, de limiter les risques et de contribuer à déceler l'intention frauduleuse de tout détenteur ou utilisateur irrégulier. Cette intention frauduleuse sera d'autant mieux caractérisée qu'existera la documentation simple et accessible qui fait aujourd'hui défaut.

1) *Cf.* rapport 2001, page 29.

Chapitre V

Actualités de l'année 2002

En début d'année, deux affaires à retentissement médiatique ont suscité l'intérêt de la Commission. La première concernait l'écoute alléguée d'un scientifique, la seconde une compromission du secret-défense par la fourniture de renseignements à un trafiquant de drogue par un fonctionnaire de police, travaillant au groupement interministériel de contrôle (GIC).

L'écoute alléguée d'un scientifique

Dans sa livraison du 11 janvier 2002, disponible la veille, l'hebdomadaire *Le Point* publiait un article intitulé « Un scientifique sous surveillance ». Les auteurs de l'article exposaient que Pierre Meneton, chercheur à l'INSERM, avait fait l'objet d'une surveillance policière, et en particulier d'écoutes administratives, en raison de ses recherches sur la nocivité du sel dans les aliments, travaux dont les conclusions étaient susceptibles de nuire à la filière agroalimentaire.

Au soutien de cette assertion était reproduit un document à en-tête du ministère de l'Intérieur, présenté comme une preuve de l'interception dont était victime le chercheur.

Les vérifications entreprises par les services intéressés, sur la base de ce document, permettaient de suspecter un faux. Sollicitée dès le 10 janvier par plusieurs médias, la Commission s'en tenait à son attitude traditionnelle de ne jamais confirmer ni infirmer une écoute, mais relevait des anomalies dans le document reproduit.

Le ministère de l'Intérieur adoptait cependant le parti du démenti formel dans l'après-midi du 10 janvier. En réaction, l'hebdomadaire mettait en

ligne sur son site web la version intégrale du document publié le matin et qui avait été tronqué pour des raisons avancées comme purement techniques.

La persistance d'anomalies sur le document présenté comme intégral déterminait le préfet de police à déposer plainte du chef de faux.

Durant la journée du 10 janvier, cette écoute supposée a mobilisé très largement radios, télévisions (interviews du président de la CNCIS et du délégué général) et presse écrite. Dès le lendemain, au vu du démenti formel et argumenté du ministère de l'Intérieur, la polémique cessait pour laisser place, pendant quelques jours, aux travaux du chercheur sur les méfaits du sel dans l'alimentation.

La protection des sources invoquée par les coauteurs de l'article amenait le procureur de la République de Paris à classer sans suite la plainte le 18 juillet 2002.

Compromission du secret-défense

Le vendredi 8 février 2002, l'agence France-Presse révélait qu'« un gardien de la paix, détaché par la brigade des stupéfiants de la préfecture de police de Paris au sein du groupement interministériel de contrôle (GIC), service des écoutes officielles, avait été interpellé puis placé en garde à vue, soupçonné d'avoir transmis des informations confidentielles à un voyou, selon des sources proches de l'enquête ».

Présenté au juge d'instruction Jean-Paul Valat, au cabinet duquel une information était ouverte, il était mis en examen le lendemain, des chefs de corruption active et passive de fonctionnaire, infraction à la législation sur les stupéfiants, violation du secret professionnel et compromission du secret-défense, et placé sous mandat de dépôt.

Lors de son interpellation, conjointement avec celle d'un délinquant notoire, il était porteur d'une liste manuscrite de numéros de téléphone susceptibles d'avoir fait l'objet d'interceptions.

Le 6 juin 2002, la Commission consultative du secret de la défense nationale saisie par le Premier ministre sur la requête du magistrat instructeur, émettait « un avis favorable à la déclassification des informations classifiées "secret-défense" afférentes à l'intégralité de la liste de numéros téléphoniques, de noms ou de prénoms, fournie par le magistrat, à l'identification des services demandeurs de ces interceptions de sécurité ainsi qu'aux dates de début et de cessation des interceptions en question » (*JO*, 3 septembre 2002, p. 14639).

Chapitre VI

Avis au Premier ministre

AVIS DU 27 NOVEMBRE 2002 SUR L'AUGMENTATION DU NOMBRE MAXIMUM D'INTERCEPTIONS DE SÉCURITÉ

La Commission a pris connaissance de l'intention du Premier ministre d'augmenter le nombre maximum des interceptions de sécurité susceptibles d'être pratiquées simultanément en application de l'article 4 de la loi du 10 juillet 1991.

La Commission a examiné les motifs qui viennent à l'appui de cette demande ainsi que du montant de la majoration envisagée.

Après délibération, la Commission a donné son accord aux chiffres proposés, à savoir un total de 1670 au lieu de 1540 dont 80 pour le ministère de l'Économie et des Finances, 1190 pour le ministère de l'Intérieur et 400 pour le ministère de la Défense.

Deuxième partie

ÉTUDES ET DOCUMENTS

Chapitre I

Présentation ordonnée des textes relatifs aux interceptions

L'ensemble des modifications législatives et réglementaires intervenues dans le domaine de l'interception ou du décryptage des données transmises par la voie des télécommunications et correspondances rend nécessaire leur présentation actualisée et exhaustive.

Les interceptions de correspondances émises par la voie des télécommunications sont de deux types, judiciaires et de sécurité. S'agissant des interceptions judiciaires, le pluriel est employé à dessein depuis l'intervention de la loi nº 2002-1138 du 9 septembre 2002.

En effet, aux interceptions en matière criminelle et correctionnelle prévues par les art. 100 et 100-7 du Code de procédure pénale, s'ajoutent désormais celles prévues par l'art. 80-4 du même Code dans le cadre de l'information ouverte pour recherche des causes de la mort ou d'une disparition de mineur, de majeur protégé ou présentant un caractère inquiétant. Avant d'exposer 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 télécommunications posé par l'article 1er de la loi nº 91-646 du 10 juillet 1991 : « Le secret des correspondances émises par la voie des télécommunications 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 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 1er)

Art. 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. «

Art. 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. »

Art. 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. »

Art. 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. »

Art. 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. »

Art. 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. »

Art 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. »

Art. 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 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

Art. 80-4 du Code de procédure pénale (loi nº 2002 -1138 du 9 septembre 2002, art. 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 1er du titre III du livre 1er. 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 de sécurité (loi nº 91-646 du 10 juillet 1991 – Titre II)

Art. 3. – Peuvent être autorisées, à titre exceptionnel, dans les conditions prévues par l'article 4, les interceptions de correspondances émises par la voie des télécommunications 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.

Art. 4. – 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 la personne que chacun d'eux aura spécialement déléguée.

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

Art. 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.

Art. 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.

Art. 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.

Art. 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.

Art. 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.

Art. 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.

Art. 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 Télécommunications ou des exploitants de réseaux ou fournisseurs des services de télécommunications autorisés ne peuvent être effectuées que sur ordre du ministre chargé des Télécommunications 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.

Art. 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.

Art. 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.

Art. 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.

Art. 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 Télécommunications.

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.

Art. 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.

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

Art. 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.

Art. 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.

Art. 19. – 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 et 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.

Dispositions communes aux interceptions judiciaires et de sécurité (loi nº 91-646 du 10 juillet 1991 – Titre III)

Art. 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.

Art. 21. – Dans le cadre des attributions qui lui sont conférées par le livre II du Code des postes et télécommunications, le ministre chargé des

Télécommunications veille notamment à ce que l'exploitant public, les autres exploitants de réseaux publics de télécommunications et les autres fournisseurs de services de télécommunications autorisés prennent les mesures nécessaires pour assurer l'application des dispositions de la présente loi.

Art. 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 télécommunications ou fournisseurs de services de télécommunications ou l'organisme visé à l'article L. 35-4 du Code des postes et télécommunications, 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 € 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.

Art. 23. – Les exigences essentielles définies au 12° de l'article L. 32 du Code des postes et télécommunications 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 Télécommunications dans l'exercice des prérogatives qui leur sont dévolues par la présente loi.

Art. 24. – *Cet article établissait une nouvelle rédaction de l'article 371 du Code pénal. Depuis l'entrée en vigueur du nouveau Code pénal, l'article 226-3 lui a été substitué.*

Article 226-3. – Est puni des mêmes peines [*un an d'emprisonnement et 45 000 € 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.

Art. 25. – *Cet article introduisait un article 186-1 dans le Code pénal. Depuis l'entrée en vigueur du nouveau Code pénal, l'article 432-9 lui a été substitué.*

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 € d'amende.

Est puni des mêmes peines le fait, par une personne visée à l'alinéa précédent ou un agent d'un exploitant de réseau de télécommunications autorisé en vertu de l'article L. 33-1 du Code des postes et télécommunications ou d'un fournisseur de services de télécommunications, 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.

L'article 25 établissait également une nouvelle rédaction de l'article L. 41 du Code des postes et télécommunications, qui a été abrogé lors de l'entrée en vigueur du nouveau Code pénal. Il a enfin abrogé l'article L 42 du Code des postes et télécommunications.

Art. 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.

Art. 27. – La présente loi entrera en vigueur le 1er octobre 1991.

Textes réglementaires récents visant la loi du 10 juillet 1991

Deux décrets méritent d'être soulignés. Le premier en date du 12 avril 2002 a trait à l'érection en service du groupement interministériel de contrôle

1) substitué dans le nouveau code pénal à l'article 378, mentionné dans la loi du 10 juillet 1991

et consacre le principe de centralisation des interceptions fixé par l'article 4 de la loi du 10 juillet 1991. Le second en date du 16 juillet 2002 tend à mettre en œuvre les obligations pesant sur les fournisseurs de prestations de cryptologie introduites par l'article 11-1 de 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 télécommunications, 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 (...)

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

Art. 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.

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

Art. 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 télécommunications (*JO* du 18 juillet 2002)

Art. 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.

Art. 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.

Art. 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.

Art. 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.

Art. 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.

Art. 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.

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

Art. 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*.

Textes récents relatifs aux télécommunications

Directive 2002/58/ce du parlement européen et du conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) [1] (extraits)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

[...]

considérant ce qui suit :

[...]

(4) La directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications a traduit les principes définis dans la directive 95/46/CE en règles spécifiques applicables au secteur des télécommunications. La directive 97/66/CE doit être adaptée à l'évolution des marchés et des technologies des services de communications électroniques afin de garantir un niveau égal de protection des données à caractère personnel et de la vie privée aux utilisateurs de

1) *JOCE*, 31.07.2002.

services de communications électroniques accessibles au public, indépendamment des technologies utilisées. Il convient, par conséquent, que ladite directive soit abrogée et remplacée par la présente directive.

(5) De nouvelles technologies numériques avancées qui posent des exigences spécifiques concernant la protection des données à caractère personnel et de la vie privée des utilisateurs sont actuellement introduites dans les réseaux publics de communications de la Communauté. Le développement de la société de l'information se caractérise par l'introduction de nouveaux services de communications électroniques. L'accès aux réseaux mobiles numériques s'est ouvert à un large public, à des conditions abordables. Ces réseaux numériques offrent de grandes capacités et de vastes possibilités pour le traitement des données à caractère personnel. Le succès du développement transfrontalier de ces services dépend en partie de la confiance qu'auront les utilisateurs que ces services ne porteront pas atteinte à leur vie privée.

[...]

(7) Dans le cas des réseaux publics de communications, il convient d'adopter des dispositions législatives, réglementaires et techniques spécifiques afin de protéger les droits et les libertés fondamentaux des personnes physiques et les intérêts légitimes des personnes morales, notamment eu égard à la capacité accrue de stockage et de traitement automatisés de données relatives aux abonnés et aux utilisateurs.

[...]

(10) Dans le secteur des communications électroniques, la directive 95/46/CE est applicable notamment à tous les aspects de la protection des droits et libertés fondamentaux qui n'entrent pas expressément dans le cadre de la présente directive, y compris les obligations auxquelles est soumis le responsable du traitement des données à caractère personnel et les droits individuels. La directive 95/46/CE s'applique aux services de communications électroniques non publics.

(11) À l'instar de la directive 95/46/CE, la présente directive ne traite pas des questions de protection des droits et libertés fondamentaux liées à des activités qui ne sont pas régies par le droit communautaire. Elle ne modifie donc pas l'équilibre existant entre le droit des personnes à une vie privée et la possibilité dont disposent les États membres de prendre des mesures telles que celles visées à l'article 15, paragraphe 1, de la présente directive, nécessaires pour la protection de la sécurité publique, de la défense, de la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) et de l'application du droit pénal. Par conséquent, la présente directive ne porte pas atteinte à la faculté des États membres de procéder aux interceptions légales des communications électroniques ou d'arrêter d'autres mesures si cela s'avère nécessaire pour atteindre l'un quelconque des buts précités, dans le respect de la Convention européenne de sauvegarde des droits de l'homme et des libertés

fondamentales, telle qu'interprétée par la Cour européenne des droits de l'homme dans ses arrêts. Lesdites mesures doivent être appropriées, rigoureusement proportionnées au but poursuivi et nécessaires dans une société démocratique. Elles devraient également être subordonnées à des garanties appropriées, dans le respect de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

(14) Par « données de localisation », on peut entendre la latitude, la longitude et l'altitude du lieu où se trouve l'équipement terminal de l'utilisateur, la direction du mouvement, le degré de précision quant aux informations sur la localisation, l'identification de la cellule du réseau où se situe, à un moment donné, l'équipement terminal, ou encore le moment auquel l'information sur la localisation a été enregistrée.

(15) Une communication peut inclure toute information consistant en une dénomination, un nombre ou une adresse, fournie par celui qui émet la communication ou celui qui utilise une connexion pour effectuer la communication. Les données relatives au trafic peuvent inclure toute traduction de telles informations effectuée par le réseau par lequel la communication est transmise en vue d'effectuer la transmission. Les données relatives au trafic peuvent, entre autres, comporter des données concernant le routage, la durée, le moment ou le volume d'une communication, le protocole de référence, l'emplacement des équipements terminaux de l'expéditeur ou du destinataire, le réseau de départ ou d'arrivée de la communication, ou encore le début, la fin ou la durée d'une connexion. Elles peuvent également représenter le format dans lequel la communication a été acheminée par le réseau.

(16) Les informations qui font partie d'un service de radiodiffusion fourni sur un réseau public de communications le sont à l'intention d'un nombre virtuellement illimité d'auditeurs et/ou de téléspectateurs et ne constituent pas une communication au sens de la présente directive. Par contre, lorsqu'il est possible d'identifier l'abonné ou utilisateur individuel qui reçoit ces informations, comme, par exemple, dans le cas de la fourniture de services vidéo à la demande, les informations acheminées s'inscrivent dans la définition de « communication » au sens de la présente directive.

[...]

(20) Il convient que les fournisseurs de services prennent les mesures appropriées pour assurer la sécurité de leurs services, le cas échéant conjointement avec le fournisseur du réseau, et informent les abonnés des risques particuliers liés à une violation de la sécurité du réseau. De tels risques peuvent notamment toucher les services de communications électroniques fournis par l'intermédiaire d'un réseau ouvert tel que l'internet ou la téléphonie mobile analogique. Il est particulièrement important que les abonnés et les utilisateurs de ces services soient pleinement informés par leur fournisseur de service des risques existants en matière de sécurité contre lesquels ce dernier est dépourvu de moyens d'action. Il convient que

les fournisseurs de services qui proposent des services de communications électroniques accessibles au public sur l'Internet informent les utilisateurs et les abonnés des mesures qu'ils peuvent prendre pour sécuriser leurs communications, par exemple en recourant à des types spécifiques de logiciels ou de techniques de cryptage. L'obligation qui est faite à un fournisseur de service d'informer les abonnés de certains risques en matière de sécurité ne le dispense pas de prendre immédiatement les mesures appropriées pour remédier à tout nouveau risque imprévisible en matière de sécurité et rétablir le niveau normal de sécurité du service, les frais en étant à sa seule charge. L'information de l'abonné sur les risques en matière de sécurité devrait être gratuite, excepté les frais nominaux qu'un abonné peut être amené à supporter lorsqu'il reçoit ou collecte des informations, par exemple en téléchargeant un message reçu par courrier électronique. La sécurité s'apprécie au regard de l'article 17 de la directive 95/46/CE.

(21) Il convient de prendre des mesures pour empêcher tout accès non autorisé aux communications afin de protéger la confidentialité des communications effectuées au moyen de réseaux publics de communications et de services de communications électroniques accessibles au public, y compris de leur contenu et de toute donnée afférente à ces communications. La législation nationale de certains États membres interdit uniquement l'accès non autorisé intentionnel aux communications.

(22) L'interdiction du stockage des communications et des données relatives au trafic y afférentes par des personnes autres que les utilisateurs ou sans le consentement de ceux-ci ne vise pas à interdire tout stockage automatique, intermédiaire et transitoire de ces informations si ce stockage a lieu dans le seul but d'effectuer la transmission dans le réseau de communications électroniques, pour autant que les informations ne soient pas stockées pour une durée plus longue que le temps nécessaire à la transmission et à la gestion du trafic et qu'au cours de la période de stockage la confidentialité des informations reste garantie. Dans la mesure où l'exige la transmission plus efficace d'informations accessibles au public à d'autres destinataires du service à leur demande, la présente directive ne fait pas obstacle à ce que ces informations soient stockées plus longtemps, à condition qu'elles soient accessibles au public en tout état de cause et sans aucune restriction et que toute donnée concernant les abonnés ou utilisateurs individuels qui les demandent soit effacée.

(23) La confidentialité des communications devrait également être assurée dans les transactions commerciales licites. Au besoin et sous réserve d'une autorisation légale, les communications peuvent être enregistrées pour servir de preuve d'une transaction commerciale. La directive 95/46/CE est applicable en pareil cas. Les parties aux communications devraient être informées de l'enregistrement avant qu'il n'ait lieu, de la ou des raisons pour lesquelles la communication est enregistrée et de la durée du stockage de l'enregistrement. La communication enregistrée devrait être effacée dès que possible et, en tout état de cause, lors de l'expiration du délai légal de recours contre la transaction.

(24) L'équipement terminal de l'utilisateur d'un réseau de communications électroniques ainsi que toute information stockée sur cet équipement relèvent de la vie privée de l'utilisateur, qui doit être protégée au titre de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Or, les logiciels espions, les pixels invisibles (*web bugs*), les identificateurs cachés et les autres dispositifs analogues peuvent pénétrer dans le terminal de l'utilisateur à son insu afin de pouvoir accéder à des informations, stocker des informations cachées ou suivre les activités de l'utilisateur, et peuvent porter gravement atteinte à la vie privée de ce dernier. L'utilisateur de tels dispositifs ne devrait être autorisée qu'à des fins légitimes, et en étant portée à la connaissance de l'utilisateur concerné.

(25) Cependant, les dispositifs de ce type, par exemple des témoins de connexion (*cookies*), peuvent constituer un outil légitime et utile, par exemple pour évaluer l'efficacité de la conception d'un site et de la publicité faite pour ce site, ainsi que pour contrôler l'identité des utilisateurs effectuant des transactions en ligne. Lorsque des dispositifs du type précité, tels que des témoins de connexion, sont destinés à des fins légitimes, par exemple faciliter la fourniture de services de la société de l'information, leur utilisation devrait être autorisée à condition que les utilisateurs se voient donner des informations claires et précises, conformément à la directive 95/46/CE, sur la finalité des témoins de connexion ou des dispositifs analogues, de manière à être au courant des informations placées sur l'équipement terminal qu'ils utilisent. Les utilisateurs devraient avoir la possibilité de refuser qu'un témoin de connexion ou un dispositif similaire soit placé sur leur équipement terminal. Ce point est particulièrement important pour les cas où des utilisateurs autres que l'utilisateur original ont accès à l'équipement terminal et donc aux données sensibles à caractère privé qui y sont stockées. L'information relative à l'utilisation de plusieurs dispositifs à installer sur l'équipement terminal de l'utilisateur ainsi que le droit de refuser ces dispositifs peuvent être offerts en une seule fois pendant une même connexion, et couvrir aussi l'utilisation future qui pourrait être faite de ces dispositifs durant des connexions subséquentes. Les méthodes retenues pour communiquer des informations, offrir un droit de refus ou solliciter le consentement devraient être les plus conviviales possibles. L'accès au contenu d'un site spécifique peut être, toutefois, subordonné au fait d'accepter, en pleine connaissance de cause, l'installation d'un témoin de connexion ou d'un dispositif analogue, si celui-ci est utilisé à ces fins légitimes.

(26) Les données relatives aux abonnés qui sont traitées dans des réseaux de communications électroniques pour établir des connexions et transmettre des informations contiennent des informations sur la vie privée des personnes physiques et touchent au droit au secret de leur correspondance ainsi qu'aux intérêts légitimes des personnes morales. Ces données ne peuvent être stockées que dans le mesure où cela est nécessaire à la fourniture du service, aux fins de la facturation et des paiements pour interconnexion, et ce, pour une durée limitée. Tout autre traitement de ces données que le fournisseur du service de communications électroniques

accessible au public peut vouloir effectuer pour la commercialisation des services de communications électroniques ou pour la fourniture de services à valeur ajoutée ne peut être autorisé que si l'abonné a donné son accord sur la base d'informations précises et complètes fournies par le fournisseur du service de communications électroniques accessible au public sur la nature des autres traitements qu'il envisage d'effectuer, ainsi que sur le droit de l'abonné de ne pas donner son consentement à ces traitements ou de retirer son consentement. Il convient également d'effacer ou de rendre anonymes les données relatives au trafic utilisées pour la commercialisation de services à valeur ajoutée, lorsque les services en question ont été fournis. Il convient que les fournisseurs de services tiennent toujours leurs abonnés informés des types de données qu'ils traitent, des finalités de ces traitements et de leur durée.

[...]

(34) Il est nécessaire, en ce qui concerne l'identification de la ligne appelante, de protéger le droit qu'a l'auteur d'un appel d'empêcher la présentation de l'identification de la ligne à partir de laquelle l'appel est effectué, ainsi que le droit de la personne appelée de refuser les appels provenant de lignes non identifiées. Dans des cas spécifiques, il est justifié d'empêcher que la présentation de l'identification de la ligne appelante soit supprimée. Certains abonnés, en particulier les services d'assistance téléphoniques et les autres organismes similaires, ont intérêt à garantir l'anonymat de ceux qui les appellent. Il est nécessaire, en ce qui concerne l'identification de la ligne connectée, de protéger le droit et l'intérêt légitime qu'a la personne appelée d'empêcher la présentation de l'identification de la ligne à laquelle l'auteur de l'appel est effectivement connecté, en particulier dans le cas d'appels renvoyés. Il convient que les fournisseurs de services de communications électroniques accessibles au public informent leurs abonnés de l'existence, sur le réseau, de l'identification des lignes appelante et connectée, ainsi que de tous les services offerts sur la base de l'identification des lignes appelante et connectée et des possibilités offertes en matière de protection de la vie privée. Cela permettra aux abonnés de choisir en connaissance de cause, parmi les possibilités qui leur sont offertes en matière de protection de la vie privée, celles dont ils souhaiteraient faire usage. Les possibilités qui sont offertes en matière de protection de la vie privée pour chaque ligne ne doivent pas nécessairement être disponibles comme un service automatique du réseau, mais peuvent être obtenues sur simple demande auprès du fournisseur du service de communications électroniques accessible au public.

(35) Dans les réseaux de communications mobiles, des données de localisation indiquant la position géographique de l'équipement terminal de l'utilisateur mobile sont traitées afin de permettre la transmission des communications. Ces données sont des données relatives au trafic couvertes par l'article 6 de la présente directive. Toutefois, les réseaux numériques mobiles peuvent aussi avoir la capacité de traiter des données de localisation qui sont plus précises que ne l'exige la transmission des communications et qui sont

utilisées pour la fourniture de services à valeur ajoutée tels que des services personnalisés d'information sur la circulation et de guidage des conducteurs. Le traitement de ces données en vue de la fourniture de services à valeur ajoutée ne devrait être autorisé que lorsque les abonnés ont donné leur consentement. Même, dans ce cas, les abonnés devraient disposer d'un moyen simple pour interdire temporairement le traitement des données de localisation et ce, gratuitement.

(36) Les États membres peuvent prévoir une limitation du droit de l'utilisateur ou de l'abonné à la vie privée en ce qui concerne l'identification de la ligne appelante lorsque cela est nécessaire pour déterminer l'origine des appels malveillants et en ce qui concerne les données d'identification et de localisation de la ligne appelante lorsque cela est nécessaire pour permettre aux services d'urgence d'intervenir le plus efficacement possible. À ces fins, les États membres peuvent adopter des mesures spécifiques autorisant les fournisseurs de services de communications électroniques à mettre à disposition les données d'identification et de localisation de la ligne appelante sans le consentement préalable de l'utilisateur ou de l'abonné concerné.

[...]

ONT ARRÊTÉ LA PRÉSENTE DIRECTIVE :

Article premier

Champ d'application et objectif

1. La présente directive harmonise les dispositions des États membres nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et des services de communications électroniques dans la Communauté.

2. Les dispositions de la présente directive précisent et complètent la directive 95/46/CE aux fins énoncées au paragraphe 1. En outre, elles prévoient la protection des intérêts légitimes des abonnés qui sont des personnes morales.

3. La présente directive ne s'applique pas aux activités qui ne relèvent pas du traité instituant la Communauté européenne, telles que celles visées dans les titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal.

Article 2

Définitions

Sauf disposition contraire, les définitions figurant dans la directive 95/46/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et les services de communications électroniques (directive « cadre ») s'appliquent aux fins de la présente directive.

Les définitions suivantes sont aussi applicables :
a) « *utilisateur* » : toute personne physique utilisant un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service ;
b) « *données relatives au trafic* » : toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation ;
c) « *données de localisation* » : toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public ;
d) « *communication* » : toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public. Cela ne comprend pas les informations qui sont acheminées dans le cadre d'un service de radiodiffusion au public par l'intermédiaire d'un réseau de communications électroniques, sauf dans la mesure où un lien peut être établi entre l'information et l'abonné ou utilisateur identifiable qui la reçoit ;
e) « *appel* » : une connexion établie au moyen d'un service téléphonique accessible au public permettant une communication bidirectionnelle en temps réel ;
f) Le « *consentement* » d'un utilisateur ou d'un abonné correspondant au « consentement de la personne concernée » figurant dans la directive 95/46/CE ;
g) « *service à valeur ajoutée* » : tout service qui exige le traitement de données relatives au trafic ou à la localisation, à l'exclusion des données qui ne sont pas indispensables pour la transmission d'une communication ou sa facturation ;
h) « *courrier électronique* » tout message sous forme de texte, de voix, de son ou d'image envoyé par un réseau public de communications qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère.

Article 3

Services concernés

1. La présente directive s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications

électroniques accessibles au public sur les réseaux publics de communications dans la Communauté.

2. Les articles 8,10 et 11 s'appliquent aux lignes d'abonnés connectées à des centraux numériques et, lorsque cela est techniquement possible et ne nécessite pas un effort économique disproportionné, aux lignes d'abonnés connectées à des centraux analogiques.

3. Lorsqu'il est techniquement impossible de se conformer aux exigences des articles 8, 10 et 11 ou lorsque cela nécessite un effort économique disproportionné, les États membres en informent la Commission.

[...]

Article 5

Confidentialité des communications

1. Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité.

2. Le paragraphe 1 n'affecte pas l'enregistrement légalement autorisé de communications et des données relatives au trafic y afférentes, lorsqu'il est effectué dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale ou de toute autre communication commerciale.

3. Les États membres garantissent que l'utilisation des réseaux de communications électroniques en vue de stocker des informations ou d'accéder à des informations stockées dans l'équipement terminal d'un abonné ou d'un utilisateur ne soit permise qu'à condition que l'abonné ou l'utilisateur, soit muni, dans le respect de la directive 95/46/CE, d'une information claire et complète, entre autres sur les finalités du traitement, et que l'abonné ou l'utilisateur ait le droit de refuser un tel traitement par le responsable du traitement des données. Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer ou à faciliter la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires à la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur.

Article 6

Données relatives au trafic

1. Les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication sans préjudice des paragraphes 2, 3 et 5, du présent article ainsi que de l'article 15, paragraphe 1.

2. Les données relatives au trafic qui sont nécessaires pour établir les factures des abonnés et les paiements pour interconnexion peuvent être traitées. Un tel traitement n'est autorisé que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement.

[...]

Article 9

Données de localisation autres que les données relatives au trafic

1. Lorsque des données de localisation, autres que des données relatives au trafic, concernant des utilisateurs ou abonnés de réseaux publics de communications ou de services de communications électroniques accessibles au public ou des abonnés à ces réseaux ou services, peuvent être traitées, elles ne le seront qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée. Le fournisseur du service doit informer les utilisateurs ou les abonnés, avant d'obtenir leur consentement, du type de données de localisation autres que les données relatives au trafic qui sera traité, des objectifs et de la durée de ce traitement, et du fait que les données seront ou non transmises à un tiers en vue de la fourniture du service à valeur ajoutée. Les utilisateurs ou les abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données de localisation autres que les données relatives au trafic.

[...]

Article 15

Application de certaines dispositions de la directive 95/46/CE

1. Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la

sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne.

2. Les dispositions du chapitre III de la directive 95/46/CE relatif aux recours juridictionnels, à la responsabilité et aux sanctions sont applicables aux dispositions nationales adoptées en application de la présente directive ainsi qu'aux droits individuels résultant de la présente directive.

3. Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, institué par l'article 29 de la directive 95/46/CE, remplit aussi les tâches visées à l'article 30 de ladite directive en ce qui concerne les matières couvertes par la présente directive, à savoir la protection des droits et des libertés fondamentaux ainsi que des intérêts légitimes dans le secteur des communications électroniques.

Article 17

Transposition

1. Les États membres mettent en vigueur avant le 31 octobre 2003 les dispositions nécessaires pour se conformer à la présente directive. Ils en informent immédiatement la Commission.

Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

2. Les États membres communiquent à la Commission le texte des dispositions de droit interne qu'ils adoptent dans le domaine régi par la présente directive, ainsi que de toute modification ultérieure de ces dispositions.

Article 18

Réexamen

Au plus tard trois ans après la date visée à l'article 17, paragraphe 1, la Commission présente au Parlement européen et au Conseil un rapport sur l'application de la présente directive et sur son impact sur les opérateurs économiques et les consommateurs, notamment en ce qui concerne les

dispositions relatives aux communications non sollicitées, en prenant en considération l'environnement international. À cette fin, la Commission peut demander des informations aux États membres, lesquelles doivent être fournies sans retard indu. Le cas échéant, la Commission soumet des propositions de modification de la présente directive, en tenant compte des conclusions du rapport susmentionné, de tout changement intervenu dans le secteur ainsi que de toute autre proposition qu'elle peut juger nécessaire afin d'améliorer l'efficacité de la présente directive.

Article 19

Abrogation

La directive 97/66/CE est abrogée avec effet à partir de la date visée à l'article 17, paragraphe 1.

Les références faites à la directive abrogée s'entendent comme étant faites à la présente directive.

Article 20

Entrée en vigueur

La présente directive entre en vigueur le jour de sa publication au *Journal officiel des Communautés européennes*.

Fait à Bruxelles, le 12 juillet 2002.

Loi 2002-1138 du 9 septembre 2002 d'orientation et de programmation pour la justice

Titre V – Dispositions relatives à l'amélioration du fonctionnement et de la sécurité des établissements pénitentiaires

Chapitre 1er – Disposition relative aux communications téléphoniques

Article 47

I. – Avant le dernier alinéa de l'article L. 33-3 du Code des postes et télécommunications, il est inséré un alinéa ainsi rédigé : « 7° les installations radioélectriques permettant de rendre inopérants dans l'enceinte des établissements pénitentiaires, tant pour l'émission que pour la réception, les appareils de télécommunications mobiles de tous types ».

II. – Dans le dernier aliéna du même article, après les mots : « mentionnées ci-dessus », sont insérés les mots : « à l'exception de celles prévues au 7° ».

Décret nº 2002-1073 du 7 août 2002 d'application de l'article 30 de la loi nº 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne et portant création du centre technique d'assistance

Le Premier ministre,
Sur le rapport du ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales,
Vu le Code pénal, notamment ses articles 413-9 et suivants ;
Vu le Code de procédure pénale, notamment ses articles 16 et 28, 60, 77-1 et 156, 230-1 à 230-3 ;
Vu la loi nº 66-492 du 9 juillet 1966 portant organisation de la police nationale ;
Vu la loi nº 90-1170 du 29 décembre 1990 modifiée sur la réglementation des télécommunications ;
Vu la loi nº 98-567 du 8 juillet 1998 instituant une Commission consultative du secret de la défense nationale ;
Vu la loi nº 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, notamment son article 30 ;
Vu le décret nº 85-1057 du 2 octobre 1985 relatif à l'organisation de l'administration centrale du ministère de l'Intérieur, modifié en dernier lieu par le décret nº 99-57 du 29 janvier 1999, notamment son article 5 ;
Vu le décret nº 2000-405 du 15 mai 2000 portant création d'un Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.

Décrète :

Art. 1er. – Il est créé au ministère de l'Intérieur un centre technique d'assistance placé sous l'autorité du directeur général de la police nationale.
Art. 2. – Le centre technique d'assistance constitue l'organisme technique visé à l'article 230-2 du Code de procédure pénale.
Art. 3. – Les opérations réalisées par le centre technique d'assistance sont couvertes par le secret de la défense nationale.
Art. 4. – Les dispositions du présent décret sont applicables dans les îles Wallis et Futuna, en Polynésie française et en Nouvelle-Calédonie.
Art. 5. – Le ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales, le garde des Sceaux, ministre de la Justice, la ministre de la Défense, le ministre de l'Économie, des Finances et de l'Industrie et la 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.

Chapitre III

Réflexions sur le motif d'interception « prévention de la criminalité et de la délinquance organisées »

Comme les chiffres l'ont encore révélé cette année et en dépit des suites de l'attentat du 11 septembre 2001 et de l'accroissement consécutif de la lutte antiterroriste, le motif principal des interceptions de sécurité est et demeure la lutte contre la criminalité et la délinquance organisées.

Certes, quelquefois, qu'il s'agisse du blanchiment d'argent à grande échelle pouvant impliquer des responsables politiques ou policiers de pays tiers, soit de réseaux de financement plus ou moins volontaire de mouvements terroristes, les trois principaux motifs d'interception, à savoir le terrorisme, la criminalité et la délinquance organisées, et la sécurité nationale pourraient être retenus. Mais dans quatre-vingt-dix pour cent des cas l'embarras du choix du motif n'existe pas : trafic de stupéfiants ou attaques de transports de fonds, il s'agit là purement et simplement de criminalité et de délinquance organisées.

Cela n'interdit pas de s'interroger un peu plus sur ce concept qui n'existe pas, du moins pas strictement à l'identique, dans le Code pénal. La CNCIS s'est naturellement déjà penchée sur la définition de ce motif (rapport 1994, page 18, et 1995, page 30). Elle a ainsi souligné que la notion de crime et délit organisés résultait tant de la définition retenue par la commission Schmelck, que de certaines dispositions du Code pénal (articles 132-71, 222-35, 224-3, 225-18, 311-9, 312,6, 313-2, 321-2, 322-8 et 442-2).

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 :
– office central pour la répression du banditisme ;
– office central pour la répression de la traite des êtres humains ;
– office central pour la répression du trafic illicite de stupéfiants ;
– office central pour la répression du faux monnayage ;
– office central pour la répression des vols d'œuvres et objets d'art [1].

L'exposé des motifs de la loi de 1991 a pour sa part retenu « le trafic illicite de stupéfiants, le grand banditisme, le trafic d'armes, de munitions, de produits explosifs et de matière nucléaire, le faux-monnayage, la grande délinquance financière, la traite des êtres humains et les vols d'œuvres et objets d'art ». Cette énumération recouvre à l'exception des trafics d'armes, munitions, explosifs et matière nucléaire, celle de la commission Schmelck.

S'agissant du Code pénal, l'article 132-71 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 ».

Les livres 2 et 4 du Code pénal précisent les infractions pour lesquelles peut-être retenue la circonstance aggravante de commission en bande organisée. Ce sont :
– la production ou la fabrication illicite de stupéfiants (art 222-35 al. 2) ;
– l'importation ou l'exportation illicite de stupéfiants (art. 222-36) ;
– l'enlèvement et la séquestration (art. 224-3) ;
– le proxénétisme déjà aggravé par d'autres circonstances (art. 225-8) ;
– le vol (art. 311-9) ;
– l'extorsion (art. 312-6) ;
– l'escroquerie (art. 313-2, 5°) ;
– le recel (art. 321-2, 2°) ;
– les destructions ou dégradations dangereuses pour les personnes (art. 322-8, 1°) [2] ;
– le transport, la mise en circulation, la détention en vue de la mise en circulation de fausse monnaie (art. 442-2).

À cette liste initiale, applicable au 1er mars 1994, ont été ajoutés depuis :
– le blanchiment (art. 324-2 tel qu'il résulte de la loi 96-392 du 13 mai 1996) ;

1) Trois offices centraux ont été créés depuis : lutte contre le trafic d'armes, d'explosifs et de matières sensibles ; contre la grande délinquance financière ; contre la cybercriminalité.
2) Par destructions ou dégradations dangereuses pour les personnes, on entend celles réalisées par l'effet d'une substance explosive, d'un incendie ou de tout autre moyen de nature à créer un danger pour les personnes.

– l'aide directe ou indirecte à l'entrée, la circulation et le séjour irréguliers (art. 21 de l'ordonnance du 2 novembre 1945 dans la rédaction issue de la loi et, encore plus récemment, l'incitation et l'aide au dopage de sportifs (art. L 3633-3 al-2 du Code de la santé publique tel qu'il résulte de la loi n° 99-223 du 23 mars 1999).

Il est à noter que les tribunaux ne font que fort peu usage des incriminations aggravées par la circonstance de commission en bande organisée à l'exception de l'escroquerie (respectivement 179, 154 et 203 condamnations en 1999, 2000 et 2001) et du recel de bien provenant d'un délit (respectivement 60, 99 et 121 condamnations en 1999, 2000 et 2001).

La caractéristique commune des infractions commises en *bande organisée* est évidemment l'aggravation de la répression, les peines encourues devenant alors généralement criminelles, contrairement à la circonstance de *réunion* qui n'aggrave que les peines correctionnelles (on reviendra plus loin sur cette distinction). Deviennent ainsi criminels :
– l'importation ou l'exportation illicites de stupéfiants dont la répression s'élève de 10 ans d'emprisonnement à 30 ans de réclusion criminelle ;
– le proxénétisme (déjà aggravé par d'autres circonstances) dont la répression s'élève de 10 ans d'emprisonnement à 20 ans de réclusion criminelle ;
– le vol dont la répression s'élève de 3 à 7 ans d'emprisonnement (selon les circonstances) à 15 ans de réclusion criminelle ;
– l'extorsion dont la répression s'élève de 7 ans d'emprisonnement à 20 ans de réclusion criminelle ;
– les dégradations dangereuses pour les personnes dont la répression s'élève de 10 ans d'emprisonnement à 20 ans de réclusion criminelle ;
– le transport, mise en circulation de fausse monnaie dont la répression s'élève de 10 ans d'emprisonnement à 30 ans de réclusion criminelle.

Dans d'autres cas (production, fabrication de stupéfiants, enlèvement et séquestration) la peine, déjà criminelle, est aggravée. Dans d'autres cas encore (blanchiment, escroquerie, recel, dopage, aide à l'immigration clandestine), les peines qui restent d'emprisonnement sont seulement aggravées.

Cependant, certaines infractions, suffisamment graves en elles-mêmes, ne sont jamais aggravées par la circonstance de commission en bande organisée. Il en est ainsi par exemple de la fabrication de fausse monnaie qui est punissable de 30 ans de réclusion criminelle. De même, le fait de diriger ou d'organiser un groupement ayant pour objet la production, la fabrication (...), l'offre, la cession de stupéfiants est puni de la réclusion criminelle à perpétuité ; mais dans ce dernier exemple la notion de direction ou d'organisation de groupement renvoie implicitement à la circonstance de bande organisée. Quant à la fabrication de fausse monnaie, on conviendra qu'elle suppose un certain degré d'*organisation* et relève par conséquent du grand banditisme traité par l'office central *ad hoc*. Elle fait donc bien partie du domaine de la criminalité ou délinquance organisées, susceptible d'interception de sécurité.

On notera encore que, si les infractions douanières de contrebande ne retiennent pas la circonstance de commission en bande organisée, il est avéré que certains trafics, de stupéfiants bien sûr mais aussi de cigarettes, d'œstrogènes, etc., sont aux mains de véritables entreprises criminelles. Les douanes disposent en revanche d'une notion beaucoup plus extensive applicable aux personnes *intéressées à la fraude* (*cf*. art. 399 du Code des douanes).

En quoi peut donc consister le caractère « organisé » de la criminalité et de la délinquance ? Ici encore le recours au Code pénal et à sa définition de la bande organisée (*cf. supra*) s'avère précieux.

Sous l'empire de l'ancien Code pénal (art. 385, tel qu'il résultait de la loi n° 81-82 du 2 février 1981, dite « sécurité et liberté »), 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, quant à eux, ont eu en tête, par le recours à la circonstance aggravante de bande organisée, 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 paraissent donc bien être des notions similaires.

La bande organisée, c'est le groupement, la réunion de plusieurs malfaiteurs. Mais quel élément constitutif au plan pénal va permettre de distinguer la commission en bande organisée de la circonstance de simple réunion ? C'est, précisément, l'*organisation* car dans la simple réunion il n'y a pas de hiérarchie, de distribution des rôles, d'entente préalable en vue de commettre des infractions. La réunion est fortuite, elle est une action collective inorganisée. La commission en bande organisée suppose nécessairement la préméditation (elle paraît également supposer un nombre de personnes, en principe supérieur à deux, chiffre qui suffit en revanche à caractériser la réunion). C'est pourquoi la circonstance de commission en bande organisée aggravera sensiblement plus les faits que la circonstance de simple réunion, certes déjà aggravante mais plus faiblement.

Au terme de cette analyse sont susceptibles d'être présentés sous le motif « criminalité et délinquance organisées », les projets d'interception de sécurité concernant :
– la production, la fabrication, l'importation, l'exportation illicites de stupéfiants et la direction de groupement d'offre ou de cession de stupéfiants ;
– l'enlèvement ou la séquestration ;
– le proxénétisme déjà aggravé par d'autres circonstances ;
– le vol, l'extorsion, l'escroquerie et le recel ;

– les destructions dangereuses pour les personnes ;
– le blanchiment ;
– la fabrication, le transport, la mise en circulation de fausse monnaie ;
– l'aide à l'entrée, à la circulation et aux séjours irréguliers d'étrangers ;
– l'incitation et l'aide au dopage de sportifs ;
– l'importation, l'exportation d'armes (au sens large), explosifs de matières nucléaires ;
– les contrebandes impliquant complicités et personnes intéressées à la fraude.

Ouvrons ici une parenthèse : c'est à une liste d'infractions similaire que parvient le Gouvernement dans le projet de loi portant adaptation des moyens de la justice à l'évolution de la criminalité. Il est, en effet, prévu d'appliquer des dispositions procédurales spéciales, notamment d'interception des correspondances émises par la voie des télécommunications, d'une part, aux crimes et délits d'association de malfaiteurs et à ceux pour lesquels est prévue la circonstance aggravée de bande organisée et, d'autre part, même en l'absence de bande organisée, aux crimes et délits suivants punis de dix ans d'emprisonnement :
– crimes et délits de trafic de stupéfiants ;
– crimes et délits d'enlèvement et de séquestration ;
– crimes et délits aggravés de proxénétisme ;
– crimes et délits aggravés de traite des êtres humains ;
– crimes et délits aggravés d'extorsion ;
– crimes et délits terroristes. On notera que le terrorisme s'éloigne ici des connotations politiques « nobles » qui pouvaient lui être attachées pour se rapprocher de la criminalité organisée dont il est une des formes, l'attentat des Twin Towers ayant démontré la capacité criminelle de groupes remarquablement organisés.

Ce projet de loi aggrave également la répression d'un nouvel ensemble d'infractions par ajout de la circonstance de criminalité organisée. Ce sont l'assassinat, les actes de tortures et de barbarie, la corruption de mineur, la diffusion d'images pornographiques de mineur, l'évasion, les délits en matière d'armes et munitions. Dans d'autres cas, enfin, c'est la répression qui est seulement accrue, la circonstance de commission en bande organisée existant déjà (*ex*. : l'escroquerie en bande organisée dont la répression est élevée de 7 à 10 ans ; la direction d'association de malfaiteurs terroriste qui est criminalisée).

Mais en s'en tenant à la première liste, tout projet d'interception concernant une autre infraction de nature criminelle qui supposerait une organisation au sens de répartition des rôles, quand bien même la circonstance de bande organisée n'aggraverait pas légalement cette infraction, pourrait être retenu.

Cette analyse pourrait se révéler précieuse par exemple dans des épisodes de violences urbaines qui ne sont pas toutes spontanées et pour lesquelles, pénalement, n'existe que la circonstance de réunion (*cf*. art. 222-8,

222-10, 222-12 et 222-13 du Code pénal ; idem pour la rébellion art 433-7 et 433-8 du même Code).

C'est ici que l'on voit que, si les deux notions « criminalité et délinquance organisées » et « infractions commises en bande organisée » paraissent similaires, elles ne sont pas pour autant identiques, la première étant sensiblement plus large. Revenons à cet égard sur la fabrication de fausse monnaie : c'est un crime passible de 30 ans de réclusion criminelle ; il relève du grand banditisme et est traité par l'office central *ad hoc* ; pour autant il n'est pas nécessairement commis en bande organisée même s'il suppose une organisation certaine. Mais celle-ci peut aujourd'hui plus résulter de la réunion de moyens techniques sophistiqués, ordinateurs, photocopieuses couleurs, etc., que du nombre de complices.

C'est pourquoi la fabrication de fausse monnaie figure bien dans l'énumération *supra*.

Et il peut être intéressant à partir de cet exemple de retenir que l'*organisation* peut, même si d'évidence cela ne peut concerner qu'un nombre limité de cas, reposer aussi bien sur les moyens matériels (et virtuels ; *cf*. la cybercriminalité) réunis que sur les seules « ressources humaines ».

En résumé et en guise de conclusion, il pourrait être avancé que tout ce qui est commis en bande organisée est nécessairement organisé, mais tout ce qui est organisé n'est pas nécessairement commis en bande organisée.

Chapitre IV

Réflexions sur le motif d'interceptions « prévention du terrorisme »

L'émergence depuis quelques années de groupes aux fondements idéologiques divers mais qui se fédèrent tous dans un violent activisme de rencontre conduit à s'interroger sur l'éventuel rattachement au terrorisme de ces agissements et à la légitimité des interceptions qui en résulteraient.

Si le terrorisme est difficile à définir au point que plusieurs auteurs préfèrent parler de terrorismes (Gérard Chaliand *in Les stratégies du terrorisme*, Desclee de Brouwer 1999 ; *Le terrorisme*, Isabelle Sommier, coll. « Dominos », 2000 ; « Un terrorisme ou des terrorismes ? », Daniel Hernant et Didier Bigo, *Esprit*, nº 94-95,1986), il est cependant possible, juridiquement, de s'appuyer sur la définition qu'en donne l'article 421-1 du Code pénal. Celui-ci définit comme actes de terrorisme un nombre limité d'infractions quand celles-ci sont « *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 prescriptions de l'action publique et de la peine ;
– les peines principales et complémentaires encourues.

Compte tenu de l'ensemble de ses dispositions dérogatoires, la qualification d'une infraction d'acte de terrorisme, au sens de l'article 421-1 du

Code pénal, revêt une particulière gravité. En effet, outre l'évidente aggravation du sort des personnes mises en cause, c'est d'un régime « abusivement » favorable dont pourraient bénéficier les victimes (régime d'indemnisation spécial ; fonds de garantie), mais surtout les complices ayant collaboré avec les enquêteurs (exemption et réduction de peine offertes aux « repentis »).

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 la circulaire crim. 86-21-F. 1 du 10 octobre 1986 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 préparé (entrepris) dans le but d'intimider ou de terroriser tout ou partie de la population.

La préparation, l'« *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 peuvent répondre à ces définitions comme l'organisation d'incidents en fin de manifestions, 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 – termes indissociables selon le garde des Sceaux de l'époque –, 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.

Yves Mayaud (*Le terrorisme, connaissance du droit*, Dalloz 1997) a confirmé à quel point l'organisation, l'acte et la finalité forment un tout indissociable et doivent être appréciés globalement pour définir ce qui relève du terrorisme.

« Qu'elle soit collective ou individuelle, l'entreprise permet de situer le comportement dans une démarche *linéaire*, à base de programmation, de mise à exécution, voire de revendication. » Le même auteur poursuit : « Qu'il n'est pas nécessaire de s'arrêter aux manifestations visibles de l'acte, voire de l'organisation qui en permet la réalisation ; il faut également remonter à la

détermination qui en a inspiré le principe afin de se convaincre que l'entreprise criminelle s'inscrit bien dans une logique d'intimidation ou de terreur. [...] (Le juge) doit toujours être guidé par la volonté de réserver la qualification terroriste aux hypothèses les plus marquantes de *déstabilisation sociale* qui ne sauraient se réduire à de simples entraves à l'exercice de l'autorité de l'État (*cf*. également crim. 14 mars 1986, *Bull. crim*., nº 123). Ce qui est en cause, c'est *l'impact* de l'entreprise terroriste, qui doit se manifester par une déstabilisation de la collectivité après avoir éveillé en elle des craintes et des angoisses dont l'effet premier est de paralyser l'esprit d'initiative, de contrarier la confiance mutuelle, et de douter des possibilités de réaction des pouvoirs publics. »

Revenant à ses premiers propos, l'auteur conclut : « Là se situe toute la finalité du terrorisme qui en fait une criminalité très particulière, à base de conception, d'organisation et de réalisation d'infraction dont l'effet doit dépasser les victimes directes, telles une *réaction en chaîne*, pour atteindre la collectivité dans son ensemble. »

Au vu de ce qui précède, n'importe quelle action d'expression ou de revendication politique, voire syndicale, violente, susceptible de troubler l'ordre public, ne saurait être qualifiée de terroriste. Il est à cet égard intéressant d'observer la réaction italienne aux mouvements violents dits « antimondialisation ». À la mi-novembre 2002, une quarantaine de dirigeants ou militants ont été inculpés sous la qualification d'« association subversive en vue de perturber les fonctions du gouvernement ». L'incrimination retenue est intéressante à plus d'un titre.

D'une part, elle témoigne de la volonté du gouvernement italien de trouver une réponse pénale à la hauteur des incidents ayant entouré le sommet de Gênes de 2001 et susceptibles de se reproduire. Cette incrimination n'a pas vraiment d'équivalent en France. Les seules qualifications proches et qui figurent au livre IV du Code pénal sont :
– le mouvement insurrectionnel (art. 412-3 du Code pénal) constitué par « toute violence collective de nature à mettre en péril les institutions de la République ou à porter atteinte à l'intégrité du territoire national », punie, selon les circonstances, de 15 à 20 ans de détention criminelle ;
– la participation délictueuse à un attroupement armé qui, après sommation, est puni de 5 ans d'emprisonnement, la provocation directe au dit attroupement étant punie de 7 ans d'emprisonnement si elle a été suivie d'effet.

D'autre part, le choix de cette incrimination signifie bien que, du point de vue italien, les actions revendicatives violentes à caractère politique ne sont pas constitutives d'actes terroristes. S'il y a bien entreprise collective ayant pour but de troubler gravement l'ordre public, manquent les éléments déterminants de la commission des actes terroristes : l'intimidation et la terreur.

En conclusion, on relèvera toutefois que, par définition, l'interception de sécurité précède la commission de l'infraction susceptible d'être qualifiée d'acte de terrorisme et que le motif prévu par la loi de 1991 est bien la

« *prévention* du terrorisme ». Dès lors, il faut bien convenir que la marge est étroite, une organisation extrémiste pouvant à tout moment s'enfermer dans une dérive de type « brigadiste », afin de se faire connaître ou reconnaître. Les pouvoirs publics qui, dans cette hypothèse, auraient renoncé à des interceptions de sécurité pourraient alors être rétrospectivement taxés d'imprévoyance.

Chapitre V

Jurisprudence européenne et française

Jurisprudence européenne

Arrêt TAYLOR-SABORI c. Royaume-Uni du 22 octobre 2002 (requête nº 00047114/99). De cet arrêt uniquement disponible en langue anglaise, il ressort que constitue une violation de l'art. 8 l'interception de messages d'un *pager* transmis par un réseau privé de radiomessagerie, alors que la loi interne ne prévoit pas ce type d'interception.

Jurisprudence française

Cour de Cassation – Chambre criminelle

Arrêt du 24 juillet 2002 :

[...] Sur le premier moyen de cassation, pris de la violation des articles 6 de la Convention européenne des droits de l'homme, 80, 100 et s. 151, 206, 591 et 593 du Code de procédure pénale ;

« en ce que la chambre d'accusation de la cour d'appel d'Aix-en-Provence, par arrêt du 22 mai 1996, a rejeté les moyens de nullité présentés par la défense ;

« aux motifs que le réquisitoire introductif du 24 septembre 1993 répond aux conditions essentielles de son existence légale ; que le versement au dossier de procédure des transcriptions d'écoutes téléphoniques issues d'un autre dossier ne peut être critiqué ; que l'information sera

poursuivie par tel juge d'instruction du tribunal de grande instance de Toulon désigné à cet effet par la chambre d'accusation ;

« alors que ne répond pas aux conditions essentielles de son existence légale le réquisitoire introductif qui ne fait pas état de faits déterminés permettant au juge d'instruction de s'assurer de sa compétence ;

« alors que la transcription d'écoutes téléphoniques irrégulièrement faites dans le cadre d'une enquête préliminaire incidente et produites – fût-ce *a posteriori* – pour "expliquer" le réquisitoire introductif prive ce dernier des conditions essentielles de son existence légale ;

« alors que méconnaît sa compétence la chambre d'accusation de renvoi désignée par la chambre criminelle "pour connaître sans limitation de l'ensemble de la procédure à l'égard de toutes les parties en cause" qui délègue la poursuite de l'instruction à un juge d'instruction près le tribunal de grande instance de son ressort » ;

Sur les première et deuxième branches ;

Attendu que les demandeurs ont soulevé la nullité du réquisitoire introductif du 24 septembre 1993 au motif que l'information a été ouverte à partir d'un compte rendu d'écoutes téléphoniques émanant d'une procédure distincte alors que ces écoutes ne figuraient pas dans la nouvelle procédure au moment de l'ouverture d'information ;

Attendu que, pour rejeter cette demande, la chambre d'accusation, statuant sur renvoi après cassation, énonce que le procureur de la République, à qui il appartient d'apprécier la suite à donner aux dénonciations qu'il reçoit, tient des articles 40, 41 et 80 du Code de procédure pénale le droit de requérir l'ouverture d'une information, au vu de simples renseignements qui ont pu lui être transmis, lorsqu'une instruction lui paraît nécessaire à la recherche et à la poursuite des infractions dénoncées ; que les juges constatent que le réquisitoire introductif comporte toutes les mentions qui le rendent régulier ; qu'ils ajoutent, en ce qui concerne les écoutes téléphoniques provenant d'une autre procédure, que celles-ci ont été régulièrement versées au dossier de l'information dans le cadre d'une expertise diligentée par le juge d'instruction le 7 décembre 1993 avant toute interpellation ;

Attendu qu'en cet état, la chambre d'accusation a justifié sa décision ;

REJETTE les pourvois ;

Décision attaquée : chambre d'accusation de la cour d'appel d'Aix-en-Provence, 1996-05-22

Cour de Cassation – Chambre criminelle

Arrêt du 9 octobre 2002 :

[...] Sur le moyen unique de cassation, pris de la violation des articles 6-1 et 8 de la Convention européenne de sauvegarde des droits de l'homme,

100-4 et 100-5 du Code de procédure pénale, 151, 152, 170, 171, 173, 174, 206, 593 et 802 du même Code, violation du principe de légalité et des articles 7 et 8 de la Déclaration des droits de l'homme et du citoyen du 26 août 1789, défaut de motifs, manque de base légale, ensemble violation des droits de la défense ;

« en ce que l'arrêt du 11 décembre 1996 attaqué a refusé d'annuler les procès-verbaux de retranscription des interceptions téléphoniques ordonnées par commission rogatoire du 17 juillet 1994 délivrée par le juge d'instruction de Grasse (cotes 1 à 28) ainsi que le réquisitoire introductif (D 103) fondé sur ces écoutes ;

« aux motifs qu'il n'appartient pas à la chambre d'accusation, dans le cadre de sa saisine, d'apprécier la régularité d'une commission rogatoire et d'actes de procédure intervenus dans le cadre d'une autre information étrangère au dossier dont elle est saisie ; que le moyen tiré de la nullité des écoutes téléphoniques et de leurs transcriptions sera donc rejeté ; qu'il n'y a pas lieu de faire droit à la demande subsidiaire de sursis à statuer dans la mesure où il n'est ni établi ni même allégué que la chambre d'accusation compétente ait été saisie d'une requête en annulation ;

« alors, d'une part, que, lorsque des poursuites judiciaires sont exclusivement fondées sur les procès-verbaux de transcription d'écoutes téléphoniques ordonnées dans une autre procédure, la personne mise en examen dans la nouvelle procédure sur le fondement exclusif de ces procès-verbaux doit avoir la possibilité – ces pièces faisant désormais partie de la nouvelle procédure – d'en demander la nullité dans les conditions des articles 170 et suivants du Code de procédure pénale ; qu'en refusant ce droit à Huy Y... au motif que la chambre d'accusation n'a pas la possibilité d'apprécier la régularité d'actes de procédure intervenus dans le cadre d'une autre procédure, la chambre d'accusation a violé les textes susvisés, et les droits de la défense ;

« alors, d'autre part, que la personne mise en examen sur le fondement de la copie de procès-verbaux de transcription d'écoutes téléphoniques ordonnées dans une autre procédure n'a pas la possibilité de déposer, dans la procédure initiale à laquelle elle est étrangère, une requête en annulation de ces actes de procédure, ni celle de provoquer un tel recours ; qu'en refusant d'examiner le moyen de nullité de Huy Y..., au motif de l'impossibilité d'appréciation de la régularité des pièces dans la nouvelle procédure, et de l'absence d'une requête en annulation dans la procédure initiale, c'est-à-dire en privant l'intéressé de toute possibilité d'obtenir un contrôle de la régularité des pièces sur lesquelles sont fondées les poursuites dirigées contre lui, la chambre d'accusation a privé l'intéressé du droit à un procès équitable, en violation de l'article 6-1 de la Convention européenne des droits de l'homme et des textes susvisés, et du droit à être jugé selon des formes légales et dont la légalité peut être contrôlée par le juge qui examine son cas, en violation des articles 7 et 8 de la Déclaration des droits de l'homme et du citoyen du 26 août 1789 » ;

Attendu qu'il résulte de l'arrêt attaqué et des pièces de la procédure, que, dans le cadre d'une information ouverte contre personne non dénommée, notamment, des chefs d'escroqueries, le placement sous surveillance de la ligne téléphonique d'une partie civile a été ordonné par le juge d'instruction ; que l'interception d'une conversation a conduit à la mise en examen dans le cadre d'une autre information, de Huy Y..., ancien compagnon de la partie civile, des chefs de vols, détention sans autorisation d'armes ou de munitions de première ou de quatrième catégorie, détention sans autorisation de substances ou d'engins explosifs ;

Attendu que, pour rejeter la requête formée par Huy Y... tendant à l'annulation du placement sur écoute de la transcription des conversations téléphoniques, l'arrêt attaqué énonce qu'il n'appartient pas à la chambre d'accusation d'apprécier la régularité d'une commission rogatoire et d'actes de procédure intervenus dans le cadre d'une information étrangère au dossier dont elle est saisie ;

Attendu qu'en prononçant ainsi, la cour d'appel a justifié sa décision ;

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

REJETTE les pourvois ;

Décision attaquée : chambre d'accusation de la cour d'appel de Paris, 1996-12-11

Cour de Cassation – Chambre criminelle

Arrêt du 30 octobre 2002 :

[...] Sur le moyen unique de cassation, pris de la violation de l'article 6.1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, ensemble violation du principe de rang constitutionnel des droits de la défense, violation des articles 116, 173 et suivants du Code de procédure pénale, méconnaissance des exigences de l'article 593 du même Code ;

« en ce que la cour, après avoir écarté le moyen tiré de la nullité de la transcription d'écoutes téléphoniques figurant sur la cote D 323, a confirmé le jugement aussi bien sur l'action publique que sur l'action douanière et a confirmé le jugement sur la peine privative de liberté prononcée, l'amende pénale et douanière, et la cour ajouta une interdiction du territoire français pour une durée de dix années ;

« au motif, propre et non contraire, que le prévenu estime que la transcription d'écoutes téléphoniques figurant sur la cote D 323 serait nulle ; malgré cette nullité, il n'en déplore pas moins qu'à une certaine époque la copie de cette transcription n'aurait pas figurée dans le double du dossier ; que la cour observe, comme le tribunal d'ailleurs, que, lors de l'audience du 15 septembre 2000, alors que le tribunal ne disposait que de la copie du

dossier d'instruction, l'original étant au greffe de la Cour de cassation, une copie conforme du procès-verbal 1903-98 a été versée au dossier ;

que, d'autre part, la cour observe que cette fameuse pièce, qui ne constitue d'ailleurs en rien la pierre angulaire de la procédure, figurait déjà dans l'original du dossier d'instruction pour la cote D 323, auquel le conseil du prévenu avait naturellement accès, et ce, depuis plusieurs mois ; or, à aucun moment, pendant l'instruction, l'annulation ou le retrait de cette pièce n'ont été sollicités, aucune critique n'a été faite alors qu'il était si facile à ce stade de la procédure de faire telle ou telle demande au soutien de ceci ou de cela ; que la cour ne voit d'ailleurs pas en quoi pourrait constituer la prétendue nullité, les discordances possibles, évoquées par le prévenu, entre des écoutes originales en langue turque, traduites en néerlandais, puis traduites de nouveau en français, ce qui n'est étayé par aucun élément, et rien ne permet de remettre en doute la validité de la transcription, telle que figurant au dossier en langue française ;

que cette transcription n'a donc pas été retirée du dossier, ce dont on ne voit d'ailleurs pas l'intérêt, dès lors que cette pièce était versée au dossier par le juge d'instruction et qui ne constitue que l'un des moyens de preuve pouvant être discuté contradictoirement, ce qui a été le cas et qui l'est toujours évidemment ; qu'enfin, et pour clore cette rubrique, il résulte des articles 116, 173 et suivants du Code de procédure pénale que les demandes de nullité ne sont plus recevables après le délai prévu ; que cette disposition a été régulièrement notifiée au prévenu et à son conseil ; que, d'ailleurs, les éventuelles nullités inexistantes en l'espèce sont purgées par ordonnance de renvoi ; le tribunal, lors de l'audience du 15 septembre 2000, avait relevé que le conseil du prévenu avait expressément déclaré qu'il était déjà en possession de la pièce en cause, s'agissant d'un procès-verbal figurant dans le dossier original ;

« alors que, d'une part, dans ses conclusions circonstanciées, l'appelant insistait sur le fait que si le procureur avait disposé de l'original (les 213 feuillets dans la cote D 323, procès-verbal n° 1903-98) pour rédiger, le 29 juin 2000, son réquisitoire définitif qui visait cette cote D 323, la juridiction du Mans l'avait adressée au greffe de la Cour de cassation saisie des deux pourvois de Métin X... du 3 juillet 2000 et que cette cote D 323 ne figurait pas dans la copie du dossier, seul disponible jusqu'alors aux parties ; qu'ainsi, le procureur du Mans a eu le mérite de demander le report de l'affaire, notamment pour faire adresser à ces contradicteurs cette cote D 323 inexistante jusqu'à cette date dans la copie du dossier ; que le jugement du 15 décembre 2000 n'a pas relevé non plus l'attestation de la conformité de la copie du dossier dont seule la juridiction disposait avec l'original, adressé à la Cour de cassation ; qu'en ne répondant pas à cette articulation essentielle et en procédant par voie d'affirmation, sans avoir procédé à la moindre vérification sur l'effectivité de la situation discutée, la Cour méconnaît les exigences de l'article 593 du Code de procédure pénale ;

« alors que, d'autre part, le prévenu faisait valoir que le procès-verbal faisait état de la transcription de conversations téléphoniques interceptées

sur écoute aux Pays-Bas et établissait que la quasi-totalité de ces conversations était menée en langue turque ; que le procès-verbal ne porte aucune traduction de la langue turque en langue néerlandaise, or, ce sont ces conversations originaires et de langue turque traduite que l'accusation oppose à Métin X... en sorte qu'il est impossible de s'assurer de la fidélité de la traduction initiale en néerlandais et effectuée aux Pays-Bas de ces conversations ; que la seule traduction en français de documents en néerlandais ne satisfait pas au droit au procès équitable institué par l'article 6 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et que les exigences d'un procès équitable ne pouvaient être sauves en l'espèce que par la production non seulement de la traduction des écoutes de langue turque en hollandais mais de la certification par un même traducteur interprète des trois langues : turc, hollandais et français, inscrit ou ayant prêté serment et assurant le tribunal et les parties en présence de l'exactitude, sinon de la régularité de la transcription des écoutes de langue turque en langue hollandaise puis de cette langue en français, seules ces dernières ayant figuré au dossier ; qu'ainsi, ne pouvant en aucun cas être utilisés en l'état par le juge, les 219 feuillets de traduction et autres qui constituent la pièce D 323 du dossier, sauf à méconnaître les exigences d'un procès équitable ;

qu'en écartant ce moyen en retenant, pour ce faire, des considérations inopérantes et évasives, la cour ne permet pas à la chambre criminelle d'exercer son contrôle au regard des exigences de l'article 6 précité, ensemble des exigences et droits de la défense ;

« et alors, enfin, que le moyen tiré de l'absence de traduction par un traducteur habilité des écoutes de la langue turque au néerlandais intéressait la question du bien-fondé d'éléments de conviction importants si bien qu'indépendamment du régime des nullités, et qui était en cause, c'était la question des éléments de conviction et leur sincérité ; qu'en n'examinant pas le litige sous cet angle, la Cour viole de plus fort les textes et le principe cités au moyen » ;

Attendu que, devant la cour d'appel, Métin X... a fait valoir, d'une part, que le procès-verbal portant transcription d'écoutes téléphoniques ne figurait pas dans le double du dossier, seul disponible lorsque l'original fut envoyé à la Cour de cassation, d'autre part, que ce procès-verbal devait être annulé en l'absence de certitude sur la fidélité de la traduction française des conversations enregistrées ;

Attendu que, pour écarter ce moyen, la cour d'appel relève, notamment, que, lors des débats qui ont eu lieu devant le tribunal correctionnel, le 15 septembre 2000, alors que cette juridiction ne disposait que de la copie du dossier d'instruction, une copie conforme du procès-verbal de transcription des écoutes téléphoniques a été versée au dossier ; que cette pièce figurait déjà dans l'original du dossier d'instruction, auquel le conseil du prévenu avait naturellement accès depuis plusieurs mois ; que, par ailleurs, les éventuelles nullités existant en l'espèce sont purgées par l'ordonnance de renvoi ;

Attendu qu'en cet état, la cour d'appel a justifié sa décision ;

[...]

REJETTE les pourvois ;

Décision attaquée : chambre d'accusation de la cour d'appel d'Angers, 2000-06-28

Cour de Cassation – Chambre criminelle

Arrêt du 20 novembre 2002 :

[...] Sur le premier moyen de cassation proposé par la société civile professionnelle Piwnica-Molinié pour Jean-Pierre X..., pris de la violation des articles 100-1, C 100-1, 174, 591, 593 et 609-1 du Code de procédure pénale, 6 et 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, défaut et contradiction de motifs, manque de base légale ;

« en ce que l'arrêt attaqué (n 986/2002) a refusé de prononcer l'annulation des surveillances téléphoniques relatives à la ligne..... attribuée à un abonné en Espagne et faisant l'objet de la procédure n° 1138 (D 572 à D 600) ainsi que les actes qui en sont la conséquence ;

« aux motifs, d'une part, que les requérants font état de discordance entre une copie certifiée conforme de la commission rogatoire du 24 juin 1997 prescrivant une autorisation d'écoute d'une durée de quinze jours et celle du procès-verbal de saisine mentionnant une autorisation d'une durée de deux mois ; qu'il convient en tout état de cause de se référer à l'original du dossier qui comporte, à la cote D 569, une commission rogatoire en date du 24 juin 1997 prescrivant la surveillance de la ligne téléphonique susvisée pour une durée de quatre mois, soit jusqu'au 24 octobre 1997 et que, dès lors, les procès-verbaux de retranscription d'écoutes téléphoniques du 27 juin 1997 (cote D 572) au 22 octobre 1997 (cote D 602) ont été établis en toute légalité ;

« aux motifs, d'autre part, qu'il est fait observer par la défense que la commission rogatoire figurant en original au dossier prévoit un délai de quatre mois alors que la copie certifiée conforme de la même commission rogatoire technique prévoit un délai de deux mois de sorte qu'un faux aurait été commis ; qu'il s'agit d'un nouveau moyen ; qu'il résulte des articles 174 et 609-1 du Code de procédure pénale que la chambre de l'instruction statuant sur renvoi après cassation partielle n'est saisie que dans la limite de la cassation prononcée et ne saurait en conséquence statuer au-delà de cette limite sans excéder ses pouvoirs et que ce moyen est en conséquence irrecevable ;

« 1) alors, que si la juridiction de renvoi ne peut statuer que sur les demandes initiales, en revanche, elle doit statuer sur tous les moyens, même nouveaux, venant au soutien de ses demandes et qu'en refusant par conséquent d'examiner l'argumentation de Jean-Pierre X... présentée au

soutien de sa demande de nullité de la surveillance de la ligne téléphonique susvisée selon laquelle l'original de la commission rogatoire en date du 24 juin 1997 qui servait de base à cette surveillance était suspect et par conséquent ne permettait pas de valider la procédure sous prétexte qu'il s'agissait d'un moyen nouveau, la cour de renvoi a violé par fausse application les dispositions combinées des articles 174 et 609-1 du Code de procédure pénale ;

« 2) alors que la chambre criminelle, à laquelle est soumise la procédure ayant fait l'objet de l'arrêt de cassation en date du 14 novembre 2001, est en mesure de s'assurer par l'examen du mémoire régulièrement déposé par les conseils de Jean-Pierre X... le 10 avril 2001 que ceux-ci avaient d'ores et déjà présenté cette argumentation au soutien de leur demande d'annulation, laquelle est demeurée inchangée et qu'en affirmant dès lors qu'il s'agissait d'un moyen nouveau, la cour de renvoi a statué par un motif qui contredit les pièces de la procédures ;

« 3) alors que la durée d'une surveillance téléphonique est, tant en application de l'article 100-1 du Code de procédure pénale qu'en application des principes déduits de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, une formalité substantielle, et que son caractère incertain entache la surveillance téléphonique de nullité et que dans la mesure où la copie certifiée conforme de la commission rogatoire en date du 24 juin 1997 revêtue du sceau du magistrat, remise aux conseils de Jean-Pierre X... et annexée à son mémoire devant la cour de renvoi indique une durée d'écoute de quinze jours, tandis que le procès-verbal de saisine daté du même jour émanant de l'officier de police judiciaire énonce une durée d'écoute de deux mois, la chambre de l'instruction ne pouvait, sans méconnaître ses pouvoirs et mieux s'expliquer, refuser d'annuler la surveillance téléphonique de la ligne susvisée » ;

Sur le second moyen de cassation proposé par la société civile professionnelle Piwnica-Molinié pour Jean-Pierre X..., pris de la violation des articles 100-1, C 100-1, 591 et 593 du Code de procédure pénale, 6 et 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ;

« en ce que l'arrêt attaqué (n 986/2002) a refusé de prononcer l'annulation des surveillances téléphoniques relatives à la ligne..... attribuée à un abonné en Espagne, faisant l'objet de la procédure nº 1226 (D 604 à D 613) et les actes de la procédure subséquents ;

« aux motifs, que la commission rogatoire en date du 30 juin 1997 (cote D 603) qui a autorisé la surveillance de la ligne téléphonique susvisée ne mentionne pas le délai durant lequel cette surveillance est autorisée ; qu'il convient de constater cependant que non seulement le délai maximum de quatre mois visé par l'article 100-2 du Code de procédure pénale n'a pas été dépassé mais que les écoutes ont été réalisées durant un délai de dix jours, du 7 juillet 1997 (cote D 606) au 17 juillet 1997 (cote D 610), qu'aucun grief ne saurait être invoqué dès lors que le délai légal n'a pas été dépassé ;

« alors, qu'il résulte de l'article 100-1 du Code de procédure pénale et des principes déduits des textes conventionnels susvisés que l'indication dans la décision qui ordonne l'interception de la durée de celle-ci est une condition essentielle de la validité de cette interception et que l'absence de cette indication fait par elle-même grief » ;

Sur le second moyen de cassation proposé par la société civile professionnelle Waquet-Farge-Hazan pour Jean-Claude Z..., pris de la violation des articles 80, 81, 100 à 107, 151, 152, 593 et 802 du Code de procédure pénale, 6 et 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, défaut de motifs, manque de base légale ;

« en ce que la chambre de l'instruction a refusé d'annuler l'intégralité des écoutes téléphoniques concernées par les demandes de Jean-Claude Z..., Franck et Pascal A..., ainsi que la procédure subséquente ;

« aux motifs, d'une part, que pour les lignes n°....., les écoutes se sont poursuivies au-delà de la date prévue par la commission rogatoire mais n'ont donné lieu à aucune retranscription postérieurement à cette même date ;

« alors que l'interception, l'enregistrement et la transcription de correspondances émises par la voie de télécommunications doivent être autorisés par le juge d'instruction et effectués sous son contrôle, étant précisé que l'interception et l'enregistrement, même en l'absence de transcription, effectués sans autorisation, portent nécessairement atteinte à la personne concernée ; qu'en admettant expressément que les écoutes et la procédure subséquente s'étaient poursuivies au-delà de la durée autorisée, tout en refusant d'annuler l'ensemble des opérations concernant les lignes n°....., au motif inopérant qu'il n'y avait pas de transcription des conversations, la chambre de l'instruction a violé les textes susvisés ;

« aux motifs, d'autre part, que pour la ligne n°....., les requérants font état d'une discordance entre une copie certifiée conforme de la commission rogatoire du 24 juin 1997 prescrivant une autorisation d'écoute d'une durée de quinze jours et celle du procès-verbal de saisine mentionnant une autorisation d'une durée de deux mois ; mais que l'original du dossier comporte, à la cote D 569, une commission rogatoire en date du 24 juin 1997 prescrivant la surveillance de la ligne téléphonique susvisée pour une durée de quatre mois, soit jusqu'au 24 octobre 1997 ;

« alors que ces énonciations procèdent d'une dénaturation des termes clairs et précis de la copie certifiée conforme de la commission rogatoire du 24 juin 1997, figurant au dossier de la chambre criminelle, dès lors qu'il y est énoncé "donne commission rogatoire à monsieur le directeur du SRPJ de Marseille à l'effet de procéder à toutes réquisitions utiles en vue de la surveillance technique, pour une durée de quinze jours, de l'abonnement téléphonique n°..... " ; que, dès lors, en considérant que cette commission rogatoire prescrivait la surveillance de la ligne téléphonique en cause

"pour une durée de quatre mois", pour rejeter la demande de nullité, la chambre de l'instruction n'a pas donné de base légale à sa décision ;

« aux motifs, enfin, que pour la ligne nº..... la commission rogatoire du 30 juin 1997 qui a autorisé la surveillance de cette ligne ne mentionne pas de délai durant lequel cette surveillance est autorisée ; mais qu'il convient de constater que le délai maximum de quatre mois n'a pas été dépassé et que les écoutes ont été réalisées durant un délai de dix jours ;

« alors, que conformément à l'article 100-1 du Code de procédure pénale, toute commission rogatoire décidée par le juge d'instruction, et prescrivant des écoutes téléphoniques, doit impérativement comporter la durée de l'interception de la ligne téléphonique en cause ; qu'il s'agit d'une mention obligatoire dont l'omission affecte nécessairement la régularité de l'autorisation et porte atteinte aux intérêts de la personne mise en examen ; qu'en admettant que la commission rogatoire en cause ne mentionnait pas le délai durant lequel la surveillance de la ligne téléphonique était autorisée, tout en refusant d'annuler les opérations d'écoute effectuées et la procédure subséquente, aux motifs inopérants que le délai légal de quatre mois n'avait pas été dépassé et, qu'en tout état de cause, les écoutes avaient uniquement été réalisées dans un délai de dix jours, la chambre de l'instruction a violé les textes susvisés » ;

Sur le quatrième moyen de cassation proposé par Me Bouthors pour Alain B..., pris de la violation des articles 80 et suivants, 100 et suivants, 151, 152, 174, 206, 591, 593 et 609-1 du Code de procédure pénale ;

« en ce que la chambre de l'instruction a écarté les moyens de nullité des commissions rogatoires techniques notamment de la commission cotée D 569 et des écoutes téléphoniques subséquentes ;

« aux motifs que, par arrêt du 7 juin 2001, la chambre de l'instruction a rejeté les moyens de nullité soulevés par les conseils de plusieurs mis en examen concernant les commissions rogatoires techniques et les écoutes téléphoniques relatives à dix lignes téléphoniques parmi lesquelles la commission rogatoire technique cotée D 569 relative à la ligne..... ; que, par arrêt du 14 novembre 2001, la chambre criminelle de la Cour de cassation a rejeté les pourvois formés à l'encontre de l'arrêt précité pour ce qui concerne les dispositions relatives aux écoutes téléphoniques énumérées, de sorte que l'arrêt de la chambre de l'instruction est définitif sur ce point et qu'il convient d'en adopter la motivation (...) qu'ainsi, les actes de procédures relatifs aux surveillances techniques et aux écoutes téléphoniques n'encourent aucune nullité à l'exception de la pièce cotée D 1106 dont la nullité a déjà été prononcée par l'arrêt du 7 juin 2001 ; (...) ; que les moyens de nullité concernant les commissions rogatoires techniques, écoutes téléphoniques consécutives et actes subséquents doivent être rejetés ; qu'il est fait observé par la défense que la commission rogatoire figurant en original au dossier prévoit un délai de quatre mois alors que la copie certifiée conforme de la même commission rogatoire technique prévoit un délai de deux mois en sorte qu'un faux aurait été commis ; qu'il s'agit d'un moyen nouveau ;

qu'il résulte des articles 174 et 609-1 du Code de procédure pénale que la chambre de l'instruction statuant sur renvoi après cassation partielle n'est saisie que dans la limite de la cassation prononcée et ne saurait en conséquence statuer au-delà de cette limite sans excéder ses pouvoirs ; que le moyen est en conséquence irrecevable ;

1) « alors que, d'une part, statuant comme juridiction de renvoi après cassation, la cour n'a pu objecter au requérant la "chose jugée" sur les moyens de nullité présentés par d'autres parties ;

2) « alors que, d'autre part, une écoute doit être limitée dans le temps par le juge et ne peut excéder la durée ainsi définie ;

qu'en refusant dès lors d'annuler les écoutes réalisées au-delà du délai prévu par le juge ou ordonnées sans limitation de duré, la cour a exposé son arrêt à la cassation ;

3) « alors que, de troisième part, la cour n'a pu légalement retenir que l'écoute de la ligne n°..... avait été ordonnée pour quatre mois quant la commission rogatoire correspondante indiquait une durée de quinze jours ;

4) « alors, en tout état de cause, que n'est pas nouveau un moyen révélé à la défense par le dossier mis à sa disposition devant la juridiction de renvoi » ;

Les moyens étant réunis ;

Attendu que, pour rejeter les moyens d'annulation visant les commissions rogatoires ordonnant des surveillances de lignes téléphoniques ainsi que les actes subséquents, la chambre de l'instruction prononce, notamment, par les motifs reproduits aux moyens ;

Attendu qu'en cet état, les griefs allégués ne sont pas encourus, dès lors que la juridiction de renvoi a répondu, à bon droit, sans insuffisance ni contradiction, aux articulations essentielles des mémoires dont elle a été saisie, dans les limites de la cassation partielle qui a été prononcée ;

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

[...]

Décision attaquée : chambre de l'instruction de la cour d'appel d'Aix-en-Provence, 2002-06-27

Questions parlementaires

Interceptions de sécurité

Développement des moyens de communication et modalités des demandes et autorisations d'écoutes téléphoniques administratives

34095 -28 juin 2001 – M. Jean-François Picheral attire l'attention de M. le Premier ministre sur les conséquences de l'accroissement des moyens de communication relatives aux modalités des demandes et autorisations d'écoutes téléphoniques administratives. Axée sur la prévention, les écoutes administratives sont soumises à des quotas fixés par vos services, et placées sous le contrôle de la Commission nationale de contrôle des interceptions de sécurité (CNCIS). Cette autorité administrative indépendante a en effet pour principale mission de vérifier la légalité des autorisations d'interception. Composée de trois membres et présidée par un conseiller d'État, la Commission a publié dernièrement son rapport annuel, qui fait état d'une diminution notable en rapport à l'année 1999-2000, tant en ce qui concerne les demandes faites par les autorités compétentes (-8,49 %), qu'au niveau des autorisations qu'elle délivre (-8,78 %). Pourtant, l'accroissement de la consommation de télécommunications, induite par la multiplicité toujours plus grande des moyens mis à la disposition du public, est, depuis quelque temps, lui aussi notable. Devant l'ouverture à la concurrence et la multiplication des moyens de communication, il lui demande donc de lui indiquer si des dispositions sont à envisager afin de répondre efficacement à ces changements techniques structurels. Ces dernières pourraient, en effet, permettre à cette Commission de faire face de manière systématique et exhaustive aux demandes, et ainsi de répondre rapidement aux nécessités de ces interceptions, tout en restant dans le respect des droits individuels des citoyens.

N. B. : l'augmentation des interceptions aux cours des années 2001 et 2002 et l'augmentation des contingents d'interception simultanées applicable en janvier 2003 constituent, à défaut de réponse officielle, quelques éléments de réponse.

Télécommunications

Internet – fournisseurs d'accès – adresses électroniques – confidentialité

787 -22 juillet 2002 – M. Jacques Myard appelle l'attention de M. le garde des Sceaux, ministre de la Justice, sur un problème qui touche de plus en plus fréquemment les utilisateurs de l'internet, celui de la réception, à leur adresse électronique, de messages à caractère pornographique. En effet, il semble que les fournisseurs d'accès à internet, notamment Wanadoo, n'offrent plus la possibilité pour leurs abonnés de s'inscrire sur des listes rouges pour leurs adresses électroniques. Les expéditeurs de messages pornographiques donnent bien la possibilité de faire radier ces adresses électroniques, en donnant accès à une adresse de désinscription, parce que la loi les y oblige, mais cliquer sur cette adresse de désinscription revient, dans les faits, à confirmer aux expéditeurs que les messages ont bien été reçus, les engageant à inonder les abonnés de nouveaux messages à caractère pornographique. C'est pourquoi il lui demande quelles mesures il envisage de prendre pour obliger les fournisseurs d'accès à l'internet à rétablir les listes rouges pour les adresses électroniques qui ne pourraient ainsi plus être communiquées sans le consentement de leurs abonnés et, également, quelles mesures il serait possible d'envisager en vue d'obliger les fournisseurs d'accès à l'internet à installer des logiciels de blocage de messages électroniques à caractère pornographique.

Réponse – Le garde des Sceaux, ministre de la Justice, fait connaître à l'honorable parlementaire que diverses mesures ont d'ores et déjà été prises permettant d'associer les fournisseurs d'accès à la protection des utilisateurs d'internet contre les messages électroniques non sollicités, notamment à caractère pornographique. Ainsi, l'article 43-7 de la loi du 30 septembre 1986 fait obligation à ces prestataires d'informer leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner ainsi que de leur proposer au moins un de ces moyens, consistant généralement en des logiciels de filtrage. À cet égard, l'association des fournisseurs d'accès (AFA) a diffusé un guide des « pratiques et usages » précisant les règles dans lesquelles s'insèrent les activités de ses membres. Il y est notamment spécifié que ces personnes doivent proposer aux utilisateurs des solutions leur permettant d'effectuer sur leur ordinateur le filtrage des contenus par des outils proposés par l'ICRA (« Internet Content Rating Association », association de classification du contenu de l'internet) ou par d'autres moyens avant même l'acheminement sur le réseau des contenus correspondants. En outre, dans

le cadre de la transposition des dispositions de la directive européenne du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, il est envisagé de subordonner l'utilisation du courrier électronique à des fins de prospection directe au consentement préalable des abonnés et non plus d'exiger de ces derniers qu'ils s'opposent à une telle utilisation. Dans ces conditions, l'édiction d'une obligation pour le fournisseur d'accès d'inscrire l'adresse électronique d'un abonné à sa demande sur une liste rouge n'apparaît pas nécessaire, d'autant que l'efficacité d'une telle mesure est limitée, compte tenu des outils multiples dont disposent les expéditeurs pour connaître l'adresse électronique d'un utilisateur d'internet.

Télécommunications (téléphone – portables – vols – lutte et prévention)

2109 -2 septembre 2002 – M. Jacques Le Nay appelle l'attention de M. le ministre de l'Économie, des Finances et de l'Industrie sur les conséquences pour les usagers de l'augmentation très nette du vol des téléphones portables enregistrée depuis l'an passé. Il lui demande de lui faire connaître les mesures urgentes qu'il compte mettre en œuvre en relation avec les trois opérateurs pour dissuader les voleurs, notamment en adoptant un système permettant de bloquer à distance l'utilisation des portables volés en empêchant leur connexion au réseau GSM.

Réponse – L'augmentation des vols des téléphones mobiles qui prend le plus souvent la forme de vol à l'arraché est une nouvelle criminalité qui constitue un véritable fait de société. L'honorable parlementaire doit être informé qu'un recensement des solutions techniques et juridiques pouvant être mises en œuvre pour lutter contre ce phénomène a été conduit dans le cadre d'un groupe de travail interministériel, regroupant les administrations concernées, les trois opérateurs de téléphonie mobile et les constructeurs de terminaux. Ce groupe de travail s'est réuni deux fois, en décembre 2001 et en janvier 2002. La solution arrêtée, comme l'évoque l'honorable parlementaire, repose sur la mise en œuvre d'une base de données relative à l'identité des terminaux volés et notamment leurs numéros « IMEI » (International Mobile Equipment Identity) ce qui permettra d'empêcher l'utilisation de ces téléphones, et pas seulement de bloquer les cartes SIM. La finalisation de ce projet est l'objet des articles 26 et 27 du projet de loi pour la sécurité intérieure, qui fait obligation aux opérateurs exploitant un réseau de radiocommunications de mettre en place, le 1er janvier 2004 au plus tard pour le territoire métropolitain, un procédé de désactivation des appareils signalés volés. S'ajoute la création d'une sanction punissant les auteurs et complices qui frauduleusement auront modifié les signes d'identification de ces appareils. Cependant, cette approche ne permettra pas de régler le problème des vols à l'arraché effectués dans le but d'utiliser le terminal volé pour passer des appels avant que le propriétaire n'ait eu le temps de déclarer le vol. Enfin, une campagne d'information est en cours sur les précautions à prendre par les utilisateurs de

terminaux de téléphonie mobile. Elle est commune à l'administration et aux opérateurs de téléphonie mobile.

Régime commun pour l'ensemble des réseaux audiovisuels et de télécommunications

2509 -19 septembre 2002 – M. Emmanuel Hamel attire l'attention de M. le ministre de la Culture et de la Communication sur le rapport de l'Autorité de régulation des télécommunications (ART) rendu public le 9 juillet dernier, analysé à la dernière page du *Figaro – Économie* du 10 juillet 2002, et dans lequel ses auteurs estiment nécessaire l'institution d'un régime commun pour l'ensemble des réseaux audiovisuels et de télécommunications « et pour la fourniture de services sur ces réseaux, quelles que soient les technologies utilisées (fixe ou mobile, filaire, hertzienne ou par satellite, réseaux câblés, etc.) ». Il lui serait reconnaissant de bien vouloir lui indiquer si des mesures allant en ce sens sont actuellement envisagées.

Réponse – L'honorable parlementaire souhaite connaître l'opinion du ministre de la Culture et de la Communication concernant la nécessité soulignée par l'Autorité de régulation des télécommunications dans son rapport annuel d'instaurer un cadre juridique unique pour l'ensemble des réseaux aussi bien de télécommunication qu'audiovisuels. Les directives européennes, parues au *Journal officiel* de l'Union européenne le 24 avril 2002, réforment le cadre juridique applicable au secteur des télécommunications en intégrant pour la première fois dans leur champ d'application, dans une notion unique de réseaux de communications électroniques, l'ensemble des réseaux audiovisuels et de télécommunication. En conséquence, le nouveau cadre harmonisé définit bien un régime juridique homogène pour les réseaux de communications électroniques. La suggestion de l'Autorité de régulation des télécommunications devrait donc être satisfaite lors de la transposition en droit national des directives avant le 24 juillet 2003. Toutefois, ainsi qu'explicitement prévu par les dispositions européennes, le champ d'application de ces textes ne couvre pas la distribution de services de communication audiovisuelle, telle qu'elle est définie par la loi du 30 septembre 1986 modifiée sur la liberté de communication, qui peut donc faire l'objet de dispositions juridiques particulières. Par ailleurs, les nouvelles dispositions européennes reconnaissent les interactions qu'il peut être nécessaire de prendre en compte entre les réseaux et les services qu'ils transportent, dans le but de ne pas porter préjudice à l'accomplissement de missions d'intérêt général, comme le pluralisme et la diversité culturelle, particulièrement dans le domaine des fréquences radioélectriques.

Transposition de la directive « Vie privée et communications électroniques »

4026 -21 novembre 2002 – M. Serge Mathieu appelle l'attention de M. le garde des Sceaux, ministre de la Justice, sur la transposition de la

nouvelle directive « Vie privée et communications électroniques », publiée au *JOCE* du 31 décembre 2002. Cette directive prévoit notamment que les envois automatisés de courriers électroniques (*e-mails*) ne seront plus autorisés, sauf exception, afin de donner un coup d'arrêt à la technique du « spam », c'est-à-dire l'envoi massif de publicités qui envahissent les boîtes aux lettres des internautes. Il souligne l'intérêt de cette directive qui, par ailleurs, prévoit d'autres dispositions dont la réglementation de l'utilisation des *cookies* afin de mieux protéger la vie privée sur internet. Il lui demande les perspectives de son action ministérielle à cet égard.

Réponse – Le garde des Sceaux, ministre de la Justice, fait connaître à l'honorable parlementaire que le Gouvernement partage son souci de voir réglementer plus efficacement la prospection électronique et ce, sachant que les communications électroniques non sollicitées constituent un phénomène dont l'ampleur a encore été dénoncée récemment par la Commission nationale de l'informatique et des libertés lors de son opération « boîte à spams ». Dans cette optique, il propose de transposer dans le projet de loi sur l'économie numérique, qui sera prochainement déposé à l'Assemblée nationale, les dispositions de la directive 2002/58 du 12 juillet 2002 relative à la vie privée et aux communications électroniques concernant l'utilisation des courriers électroniques à des fins de prospection directe. Dans le respect des termes de la directive, ce projet pose le principe de l'interdiction de la prospection au moyen de courriers électroniques de toute personne physique ou morale qui n'aurait pas exprimé son consentement préalable à recevoir de tels courriers. Par dérogation, il prévoit la possibilité pour les prestataires d'exploiter les coordonnées électroniques obtenues directement d'un client dans le cadre de la vente d'un produit ou d'un service sous réserve de porter exclusivement sur des biens ou produits analogues à ceux fournis antérieurement et que le destinataire dispose d'une faculté d'opposition. Les dispositions proposées visent enfin à interdire d'émettre des messages électroniques à des fins de prospection directe en camouflant ou en dissimulant l'identité de l'émetteur au nom duquel la communication est émise ou de mentionner un objet sans rapport avec la prestation ou le service proposé. Ce dispositif devrait permettre d'apporter une protection plus efficace des internautes contre les communications électroniques non sollicitées et renforcer en cela les dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, laquelle interdit notamment toute collecte de données nominatives par un moyen frauduleux et tout traitement automatisé de ces informations dans des conditions illicites.

N. B. : la directive visée a été publiée en réalité le 31 juillet 2002.

Terrorisme – Criminalité organisée

Criminalité organisée – blanchiment

35330-27 septembre 2001 – M. Michel Doublet attire l'attention de M^me^ le garde des Sceaux, ministre de la Justice, sur la création d'un espace judiciaire européen pour lutter de manière efficace contre « l'argent sale », notamment lié au terrorisme international, et sur le renforcement de la coopération judiciaire tant au niveau de l'Union européenne que sur le plan international. Les récents attentats survenus aux États-Unis ont créé une situation nouvelle, mettant en exergue l'urgence de la mise en place d'une conférence internationale, demandée depuis 1996 par plusieurs magistrats européens dans l'appel de Genève, et visant à éditer de nouvelles règles en matière de transparence financière, de secret bancaire, etc. En conséquence, il lui demande quelles mesures le Gouvernement compte mettre en œuvre en la matière.

Réponse – La garde des Sceaux, ministre de la Justice, fait connaître à l'honorable parlementaire que la lutte contre le blanchiment de l'argent sale a toujours été une priorité pour le Gouvernement, avant même les attentats terroristes du 11 septembre 2001. Cette détermination, affichée de longue date, a conduit la France à engager et à soutenir de nombreuses initiatives sur le plan international pour renforcer la coopération dans la lutte contre cette forme de criminalité, particulièrement lorsque celle-ci est liée au terrorisme international. Ainsi, dans le prolongement du Conseil européen de Tampere, La France avait déposé un projet de convention, transformé ultérieurement en protocole à la convention du 29 mai 2000 relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne. Ce texte, adopté par le conseil justice/affaires intérieures le 16 octobre 2001, permettra, en complétant les dispositions existantes, de lever un certain nombre d'obstacles à l'entraide judiciaire constatés par les magistrats chargés de lutter contre la criminalité financière. Il facilitera l'obtention d'informations en matière bancaire, telles que la liste des comptes détenus par une personne, le détail des opérations et la surveillance des opérations effectuées sur ces comptes. Il réaffirme également l'inopposabilité du secret bancaire et du motif fiscal, pose un principe de dépolitisation et met en place des mécanismes permettant de décourager les refus d'exécution. S'agissant plus spécialement de la lutte contre le blanchiment, le Conseil de l'Union européenne a adopté le 26 juin 2001 une décision-cadre, déposée à l'initiative de la France, qui généralise et étend l'infraction de blanchiment et instaure une harmonisation minimale des sanctions encourues. Elle améliore également le fonctionnement de l'entraide judiciaire dans ce domaine en limitant les motifs de refus de coopération en matière de dépistage, d'identification, de gel ou de saisie des produits d'infractions graves et étend l'obligation de prévoir la confiscation des instruments et des produits du crime. Par ailleurs, la France participe très activement aux travaux engagés au sein de l'Union européenne visant à mettre un terme à l'utilisation abusive des sociétés écrans et des entités juridiques opaques telles

que les trusts, les fiducies et les fondations, notamment par les groupes terroristes et la criminalité organisée, pour compliquer, voire rendre impossible, l'identification des ayants droit économiques réels. Sur la base des orientations définies par le Conseil européen de Tampere et réaffirmées pendant la présidence française par le Conseil Écofin/Jai du 17 octobre 2000, la Commission européenne a conduit une étude dont les conclusions, comportant plusieurs recommandations, ont récemment été communiquées aux États membres. La France soutient fortement le développement de ces travaux et a déjà rappelé sa volonté d'augmenter la transparence des entités juridiques à divers niveaux, financier, comptable et juridique, pour assurer l'identification des ayants droit économiques et améliorer la traçabilité des opérations financières. La nécessité de lutter contre le financement du terrorisme rend cette exigence encore plus actuelle. L'ensemble de ces initiatives contribue directement à la construction de l'espace judiciaire européen, à laquelle concourt également l'adoption des instruments permettant la mise en place d'Eurojust et du mandat d'arrêt européen. Ces instruments, quoique ayant une portée plus générale, s'appliqueront naturellement à la lutte contre le blanchiment et le financement du terrorisme. Sur le plan international, il convient de rappeler que la convention des Nations unies contre la criminalité transnationale organisée, signée par la France à Palerme, le 12 décembre 2000, contient également certaines dispositions dont la mise en œuvre favorisera la lutte contre la blanchiment, notamment par l'obligation d'incriminer de tels agissements, l'adoption de dispositifs appropriés de prévention et de détection et le développement de la coopération judiciaire en matière pénale, pour laquelle la convention réaffirme l'inopposabilité du secret bancaire. Le Gouvernement vient d'engager le processus de ratification de cet instrument majeur. Ces efforts rejoignent ceux développés par d'autres enceintes, avec le soutien très actif de la France. Le GAFI, notamment, s'est engagé dans un processus de révision des quarante recommandations qui intègre le besoin d'élaborer des normes spécifiques pour mieux lutter contre l'opacité de certaines entités juridiques utilisées aux fins de blanchiment. S'agissant plus spécialement de la lutte contre le financement du terrorisme, à laquelle le mandat du GAFI a été étendu, cette instance a adopté, le 30 octobre dernier, un ensemble de recommandations spécifiques qui prolongent les instruments existants, en particulier la convention des Nations unies contre le financement du terrorisme, d'initiative française. Ainsi qu'il est permis de le constater, de nombreuses enceintes internationales, dans le cadre de leurs compétences respectives, permettent le développement d'initiatives visant à la mise en œuvre de dispositifs efficaces de lutte contre le blanchiment et d'amélioration de la coopération judiciaire pénale, y compris dans le domaine du financement du terrorisme. Ces initiatives, qui visent à l'adoption de mesures concrètes et opérationnelles, rejoignent celles développées en matière de lutte contre le financement du terrorisme par le Conseil de sécurité des Nations unies, notamment à la suite de l'adoption de la résolution 1373, et par le G 8, tant dans ce domaine que dans celui de la coopération judiciaire. Elles reçoivent le soutien et l'appui déterminés de la France.

Terrorisme – criminalité organisée

1496 -1er août 2002 – M. René Trégouët rappelle à l'attention de M. le garde des Sceaux, ministre de la Justice, la nomination récente d'un représentant de la France auprès de l'unité de coopération judiciaire Eurojust. Peut-il lui rappeler le rôle exact qui sera le sien au sein de cet organisme ainsi que la durée de son mandat ? Peut-il lui présenter à cette occasion un bilan de l'activité de cet organisme pour l'année 2001 ?

Réponse – Le garde des Sceaux, ministre de la Justice, a l'honneur de faire connaître à l'honorable parlementaire que sa question a retenu toute son attention. Pour décrire le rôle du membre national français au sein d'Eurojust, il est nécessaire, au préalable, de rappeler l'organisation et les missions de cette unité. La création d'Eurojust a été décidée lors du Conseil européen réuni à Tampere au mois d'octobre 1999, afin de renforcer la coopération judiciaire en matière pénale entre les États membres de l'Union européenne. Eurojust n'a toutefois pas vocation à traiter toutes les affaires qui seraient susceptibles d'avoir une dimension transnationale. Sa compétence est limitée aux formes les plus graves de la criminalité organisée, comme le terrorisme, le trafic de stupéfiants ou le blanchiment des produits du crime. Comme Europol, Eurojust n'a pas compétence pour effectuer lui-même des actes d'enquête. Eurojust n'est pas un parquet européen, mais un outil de coopération dont la mission principale est de coordonner l'action des autorités nationales chargées des enquêtes et des poursuites. Il peut ainsi demander à ces autorités d'entreprendre une enquête ou d'engager des poursuites, de se dessaisir au profit d'une autre autorité ou de mettre en place des équipes communes d'enquête. Les autorités judiciaires nationales conservent néanmoins la maîtrise de l'action publique, puisqu'elles ont toujours la possibilité de rejeter la demande qui leur est adressée. Eurojust contribue, par ailleurs, à faciliter la coopération entre ces autorités en transmettant les demandes d'entraide judiciaire, ainsi que toute information utile sur les enquêtes en cours. Toutes ces missions sont effectuées en relation étroite avec Europol, l'Office européen de lutte antifraude (Olaf) et le réseau judiciaire européen. Ce réseau, qui a été spécialement créé en 1998 pour faciliter la coopération judiciaire, est constitué d'environ deux cents points de contact répartis sur l'ensemble du territoire de l'Union, qui diffusent des informations juridiques et pratiques, et qui peuvent, le cas échéant, servir d'intermédiaire entre les autorités judiciaires locales. Il existe en France un point de contact par cour d'appel, ainsi que trois points de contact nationaux.

N. B. : il est intéressant de noter que cette réponse classe le terrorisme au titre des formes les plus graves de la criminalité organisée.

Chapitre VII

Les interceptions de communications en Belgique : évolutions récentes

Le droit positif

La seule source légale d'interception est judiciaire. Le juge d'instruction ou, en cas d'urgence, un magistrat du ministère public peut, à titre exceptionnel, autoriser une écoute qui a pour objectif d'obtenir la preuve d'une infraction grave ou la participation à une telle infraction. Le repérage judiciaire (localisation et destination des appels) est par ailleurs prévu par l'article 88 bis du Code d'instruction criminelle.

En dehors de ces dispositions, seul le Service général du renseignement et de la sécurité des forces armées peut, à des fins militaires, légalement effectuer des interceptions de radiocommunications militaires émises à l'étranger (art. 44 de la loi du 30 novembre 1998 organique des services de renseignements et de sécurité).

Les évolutions en cours

Article 44 de la loi du 30 novembre 1998 : le comité permanent de contrôle des services de renseignements dit « comité permanent R » a approuvé en mai 2001 un avant-projet de loi modifiant l'article 44 de la loi du 30 novembre 1998 précitée. Cet avant-projet élargit l'exception créée au profit du Service général du renseignement et de la sécurité des forces

armées à toute forme de communication afin d'assurer, d'une part, la sécurité des troupes et celle de leurs partenaires au cours d'opérations extérieures et, d'autre part, la protection des ressortissants belges établis à l'étranger. La modification proposée « a pour objectif de répondre à l'évolution technique rapide qui permet à des individus et groupes actifs à l'étranger, des groupes cibles des services de renseignement, de ne pas hésiter à recourir aux moyens de communication modernes, tels que les téléphones portables, la correspondance électronique ou la communication par satellites, souvent associés à l'utilisation de moyens cryptographiques puissants » (chambre, 3e session de la 50e législature, 1er octobre 2001).

La modification législative approuvée par le Conseil des ministres à l'automne 2001 a été adoptée par le Parlement fin 2002.

Interceptions de sécurité

Celles-ci ne sont donc pas autorisées contrairement aux dispositions prises dans la majeure partie des autres États européens.

À la suite des événements du 11 septembre 2001, la question des interceptions de sécurité dans le cadre de la recherche proactive de renseignements en matière de lutte contre le terrorisme et la criminalité organisée a toutefois été soulevée à nouveau.

« La sûreté de l'État réclame à nouveau des compétences en matière d'écoute et d'enregistrement des télécommunications privées. Cela ne peut se faire actuellement, dans la phase de réaction, qu'en présence d'un juge d'instruction. La question de l'utilisation proactive des écoutes téléphoniques a de forts relents politiques et doit faire l'objet d'une nouvelle discussion. La mission de la sûreté de l'État consiste en effet à recueillir et analyser des informations afin de garantir la sécurité de l'État. Il faut un débat parlementaire où l'on mettrait en balance les libertés garanties essentielles telles que le droit à la vie privée, d'une part, et d'éventuelles atteintes à l'ordre public, d'autre part. Il s'agit d'un problème qui concerne typiquement le parlement. Le ministre de la Justice ne peut décider seul » (déclaration du ministère de la Justice, le 2 octobre 2001).

Le comité permanent R a recommandé que les services de renseignements puissent disposer d'un outil légal en la matière (rapport d'activité 2000 du comité permanent R, p. 56). Parallèlement, en novembre 2001, le Conseil des ministres a approuvé un projet de loi sur les techniques policières spéciales de recherche en matière de lutte contre la criminalité organisée de nature à permettre l'interception de toute forme de télécommunications (ligne classique, GSM et même écoute par microphone). Le texte a été adopté depuis par la Chambre des représentants et le Sénat.

Dans son rapport 2001 publié le 17 avril 2002, le comité permanent de contrôle des services de renseignement a fait des propositions pour une

législation belge en matière d'interception de sécurité. Le comité permanent R, s'inspirant de son étude comparative des systèmes européens et des États-Unis, a estimé que les interceptions de sécurité devraient répondre aux critères suivants :
– une demande écrite et motivée des chefs des services de renseignement et de sécurité adressée au ministre de tutelle du service, ainsi qu'éventuellement au Premier ministre ;
– une autorisation écrite d'un des ministres ou d'un secrétaire d'État délégué, pour une durée limitée renouvelable ;
– la mise en place d'une procédure d'urgence (compétence des chefs de service avec régularisation de la procédure dans un certain délai) ;
– la limitation des motivations en se référant aux missions légales des services de renseignement (ou à certaines d'entre elles comme le terrorisme et la criminalité organisée) et la justification de la mesure d'interception (subsidiarité) ;
– la notification des autorisations à un organe de contrôle parlementaire ou dépendant du parlement dans un certain délai ;
– un organe de contrôle pouvant intervenir dès le début de la procédure, en cours de celle-ci et *a posteriori*, soit d'initiative, soit sur plainte de personnes physique ou morale ; un rapport périodique devrait être adressé au parlement et aux ministres concernés ;
– une procédure d'information de la personne sur la base du modèle allemand (avec la possibilité de ne pas y procéder pour des justes motifs, avec l'autorisation de l'organe de contrôle) ;
– techniquement, la réalisation pratique de ces interceptions pourrait s'effectuer à l'initiative de l'unité globale d'interception (équivalent du GIC français) par laquelle tous les opérateurs devront passer.

Chapitre VIII

Actualités européennes

Outre la directive 2002/58 du 12 juillet 2002 (vie privée et communications électroniques ; *cf*. le présent rapport, 2e partie, chapitre II) l'actualité européenne a été marquée par l'adoption, le 15 juillet 2002, par les délégués des ministres des Affaires étrangères des 44 États membres du Conseil de l'Europe, de *lignes directrices* sur les droits de l'homme et la lutte contre le terrorisme, premier texte international dans ce domaine.

Ces lignes directrices ont été dégagées dans le rapport final du groupe de spécialistes constitué au sein du comité directeur pour les droits de l'homme. Ce groupe a remis son rapport final, le 3 juillet 2002.

Deux des lignes directrices du rapport (annexe II, chapitres V et VI) concernent la collecte et le traitement de données à caractère personnel par toute autorité compétente en matière de sécurité de l'État et les mesures d'ingérence dans la vie privée. Elles sont nourries des principes dégagés par la jurisprudence de la Cour européenne des droits de l'homme.

V – Collecte et traitement de données à caractère personnel par toute autorité compétente en matière de sécurité de l'État

Dans le cadre de la lutte contre le terrorisme, la collecte et le traitement de données à caractère personnel par toute autorité compétente en matière de sécurité de l'État ne peuvent porter atteinte au respect de la vie privée des personnes que si la collecte et le traitement sont, notamment :
1) régis par des dispositions appropriées en droit interne ;
2) proportionnés à l'objectif pour lequel cette collecte et ce traitement ont été prévus ;
3) susceptibles d'un contrôle par une autorité externe indépendante.

17. En matière de traitement de données à caractère personnel, la Cour a statué pour la première fois de la façon suivante :
« Or, aucune disposition du droit interne ne fixe les limites à respecter dans l'exercice de ces prérogatives. Ainsi, la loi interne ne définit ni le genre d'informations pouvant être consignées, ni les catégories de personnes susceptibles de faire l'objet des mesures de surveillance telles que la collecte et la conservation de données, ni les circonstances dans lesquelles peuvent être prises ces mesures, ni la procédure à suivre. De même, la loi ne fixe pas des limites quant à l'ancienneté des informations détenues et la durée de leur conservation.
(...)
La Cour relève que cet article ne renferme aucune disposition explicite et détaillée sur les personnes autorisées à consulter les dossiers, la nature de ces derniers, la procédure à suivre et l'usage qui peut être donné aux informations ainsi obtenues.
(...) Elle note aussi que, bien que l'article 2 de la loi habilite les autorités compétentes à autoriser les ingérences nécessaires afin de prévenir et contrecarrer les menaces pour la sécurité nationale, le motif de telles ingérences n'est pas défini avec suffisamment de précision « (arrêt Rotari c. Roumanie, 4 mai 2000, §§ 57-58).

VI – Mesures d'ingérence dans la vie privée

1. Les mesures dans la lutte contre le terrorisme qui constituent une ingérence dans la vie privée (notamment, les fouilles, les perquisitions, les écoutes, y compris téléphoniques, le contrôle de la correspondance et l'infiltration d'agents) doivent être prévues par la loi. Ces mesures doivent pouvoir faire l'objet d'un contrôle juridictionnel.

18. La Cour admet que la lutte contre le terrorisme permet l'utilisation de méthodes spécifiques :
« Les sociétés démocratiques se trouvent menacées de nos jours par des formes très complexes d'espionnage et par le terrorisme, de sorte que l'État doit être capable, pour combattre efficacement ces menaces, de surveiller en secret les éléments subversifs opérant sur son territoire. La Cour doit donc admettre que l'existence de dispositions législatives accordant des pouvoirs de surveillance secrète de la correspondance, des envois postaux et des télécommunications est, devant une situation exceptionnelle, nécessaire dans une société démocratique à la sécurité nationale et/ou à la défense de l'ordre et à la prévention des infractions pénales » (arrêt Klass et autres c. Allemagne, 6 septembre 1978, série A, n° 28, § 48).

19. En ce qui concerne les écoutes, il faut qu'elles soient conformes aux dispositions de l'article 8 de la Convention, notamment qu'elles soient prévues par la « loi ». La Cour a ainsi rappelé :
« Les écoutes et autres formes d'interception des entretiens téléphoniques représentent une atteinte grave au respect de la vie privée et de la

correspondance. Partant, elles doivent se fonder sur une "loi" d'une précision particulière. L'existence de règles claires et détaillées en la matière apparaît indispensable, d'autant que les procédés techniques ne cessent de se perfectionner » (arrêts Kruslin et Huvig précités, p. 23, § 33, et p. 55, § 32, respectivement ; Kopp c. Suisse, 25 mars 1998, § 72. Voir aussi Huvig c. France, 24 avril 1990, §§ 34-35).

20. La Cour a également admis que l'usage d'informations confidentielles est essentiel pour combattre la violence terroriste et la menace qui pèse sur les citoyens et sur toute la société démocratique :
« La Cour rappelle tout d'abord qu'elle reconnaît que l'utilisation d'informations confidentielles est primordiale pour combattre la violence terroriste et la menace que le terrorisme organisé constitue pour la vie des citoyens et pour la société démocratique dans son ensemble (voir aussi l'arrêt Klass et autres c. Allemagne du 6 septembre 1978, série A, nº 28, p. 23, par. 48). Cela ne signifie pas, toutefois, que les autorités d'enquête aient carte blanche, au regard de l'article 5 (art. 5), pour arrêter des suspects afin de les interroger, à l'abri de tout contrôle effectif par les tribunaux internes ou par les organes de contrôle de la Convention, chaque fois qu'elles choisissent d'affirmer qu'il y a infraction terroriste » (*Ibidem*, p. 23, par. 49 ; Murray c. Royaume-Uni, 28 octobre 1994, § 58).

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
Financement 11
Fonctionnement 11

Chapitre II
Le contrôle des autorisations 13
Les modalités du contrôle 13
Tableaux annexes 19

Chapitre III
Le contrôle de l'exécution 25
Enregistrement, transcription et durée des interceptions 25
Le contrôle du GIC 26
Les visites sur terrain 27
Réclamations de particuliers et dénonciation à l'autorité judiciaire 29

Chapitre IV
Le contrôle du matériel 31

Chapitre V
Actualités de l'année 2002 35
L'écoute alléguée d'un scientifique 35
Compromission du secret-défense 36

Chapitre VI
Avis au Premier ministre 37

Deuxième partie
ÉTUDES ET DOCUMENTS 39

Chapitre I
Présentation ordonnée des textes relatifs aux interceptions 41
Les interceptions ordonnées par l'autorité judiciaire 42
Les interceptions de sécurité (loi n° 91-646 du 10 juillet 1991 – Titre II) 44
Dispositions communes aux interceptions judiciaires et de sécurité (loi n° 91-646 du 10 juillet 1991 – Titre III) 47
Textes réglementaires récents visant la loi du 10 juillet 1991 49

Chapitre II
Textes récents relatifs aux télécommunications 53
Directive 2002/58/ce du parlement européen et du conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (extraits) 53
Loi 2002-1138 du 9 septembre 2002 d'orientation et de programmation pour la justice 64
Décret n° 2002-1073 du 7 août 2002 d'application de l'article 30 de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne et portant création du centre technique d'assistance 65

Chapitre III
Réflexions sur le motif d'interception « prévention de la criminalité et de la délinquance organisées » 67

Chapitre IV
Réflexions sur le motif d'interceptions « prévention du terrorisme » . 73

Chapitre V
Jurisprudence européenne et française 77
Jurisprudence européenne 77
Jurisprudence française 77

Chapitre VI
Questions parlementaires 89
Interceptions de sécurité 89
Télécommunications 90
Terrorisme – Criminalité organisée 94

Chapitre VII
Les interceptions de communications en Belgique : évolutions récentes 97
Le droit positif 97
Les évolutions en cours 97
Interceptions de sécurité 98

Chapitre VIII
Actualités européennes 101
V – Collecte et traitement de données à caractère personnel par toute autorité compétente en matière de sécurité de l'État 101
VI – Mesures d'ingérence dans la vie privée 102