Sommaire

Avant-propos

Le bilan de l'année 2000, établi par le présent rapport, fait d'abord ressortir une particularité touchant au nombre des interceptions de sécurité rapporté à celui des moyens de télécommunication. Il ne peut y avoir corrélation puisque le premier est limité par une décision du Premier Ministre dont la plus récente date de 1997. Mais sous le plafond ainsi fixé, l'évolution des interceptions obéit à sa logique propre, et non à l'évolution du parc de téléphones : de 1999 à 2000, celui-ci est passé – du seul fait du nombre des portables – de 54 700 000 à 63 700 000 appareils. Dans le même temps, le nombre des interceptions a baissé de 9,5 % et celui des renouvellements d'interception de 7 %. Moindre pression des menaces, pratique suivie par les services demandeurs, comportement des autorités de contrôle et de décision : tous ces facteurs ont dû jouer leur rôle dans cette évolution, mais dans une mesure difficile à déterminer.

Plusieurs des développements du rapport sont consacrés à des questions juridiques. On trouvera ci-après une présentation synthétique de la jurisprudence de la Cour européenne des droits de l'Homme en matière d'interceptions téléphoniques, jurisprudence qui est directement à l'origine de la loi du 10 juillet 1991. Il est rendu compte, par ailleurs, de la première décision du Conseil d'État sur la CNCIS, portant sur les conditions dans lesquelles celle-ci peut vérifier si une interception de sécurité est effectuée dans le respect des dispositions de la loi.

Enfin, le chapitre consacré aux opérateurs rappelle le dispositif juridique en vertu duquel ils ont l'obligation légale de satisfaire aux demandes des services compétents de l'État, moyennant, dit l'article L 35-6 du code des postes et télécommunications, une « juste rémunération ». Cette dernière règle a reçu, dans une autre formulation, la sanction constitutionnelle par la décision du Conseil constitutionnel sur la deuxième loi de finances rectificative pour 2000.

Si le contrôle de la décision par la CNCIS a un caractère exhaustif en vertu de la loi elle-même, celui de l'exécution ne peut relever que de la méthode du sondage. Pour renforcer son efficacité, il a été décidé, d'une part d'accroître le nombre de ces contrôles – qui ont porté sur 25 sites d'interception en 2000 – et d'en effectuer un certain nombre à l'improviste, ce qui fut le cas pour 12 de ces sites. Quelle que soit la méthode employée, les visites rendues aux échelons locaux sont toujours fructueuses, aussi bien pour la CNCIS que pour les services contrôlés.

Nota bene : pour éviter toute ambiguïté, on emploiera ci-après le sigle « CNCIS » pour désigner l'organisme, et on réservera le mot « Commission » à la formation composée du président, du député et du sénateur.

Première partie

RAPPORT D'ACTIVITÉ

Chapitre I

Organisation et fonctionnement de la Commission

Composition de la Commission

La composition de la commission nationale de contrôle des interceptions de sécurité n'a connu aucune modification au cours de l'année 2000. Elle se présente de la façon suivante :

Dieudonné Mandelkern, conseiller d'État, nommé à compter du 1er octobre 1997 par le Président de la République pour une durée de 6 ans, président ;
Jean-Michel Boucheron, député (PS) d'Île-et-Vilaine, nommé par le président de l'Assemblée Nationale à compter du 3 juillet 1997 pour la durée de la législature ;
Pierre Fauchon, sénateur (UDR-UC) du Loir-et-Cher, nommé par le président du Sénat à la suite du renouvellement partiel du Sénat de 1998.

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

Michèle Salvat, déléguée générale depuis sa nomination en date du 19 septembre 1997,
Laurent Becuywe, chargé de mission depuis le 3 mai 1999.
Le secrétariat est assuré par Josiane Meurice et Françoise Ferbert.

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 2000 les crédits votés représentent 2 282 776 francs dont 1 650 440 francs au titre des frais de personnel et 626 336 francs au titre des frais de fonctionnement. En application de l'arrêté du 30 avril 2000 relatif au report des crédits, la Commission a bénéficié sur son budget 2000 d'un report de 45 869 Francs au titre des rémunérations et frais de personnel, 116 689 francs au titre des prestations sociales et 65 835 francs au titre des dépenses de fonctionnement.

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 a remis le rapport annuel d'activité de la commission nationale de contrôle des interceptions de sécurité pour 1999 au Premier ministre le 5 juin 2000 et l'a présenté à la presse le 8 juin 2000.

* * *

Il apparaît à l'expérience que la composition très restreinte de la Commission, telle qu'elle est fixée par l'article 13 de la loi du 11 juillet 1991, peut nuire à son fonctionnement. Outre le président, la Commission comprend en effet « 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 ». Le même article dispose par ailleurs que, « en cas de partage des voix, la voix du président est prépondérante ». S'il advient que l'un des deux parlementaires soit absent, la Commission peut sans doute se réunir, mais il faut reconnaître que l'équilibre institutionnel voulu par le législateur n'est plus assuré, et d'autre part que l'utilisation par le président de sa voix prépondérante priverait la réunion de son sens.

La solution pourrait être d'augmenter l'effectif de la Commission pour le porter à cinq membres, comme l'a fait la loi du 8 juillet 1998 instituant une commission consultative du secret de la Défense nationale. Selon l'article 2 de cette loi, les deux membres autres que ceux représentant les assemblées sont désignés dans les mêmes conditions que le président de la Commission, c'est-à-dire par le président de la République sur des propositions faites par les chefs des plus hautes instances ou juridictions.

Colloques – séminaires – conférences

Le président de la CNCIS est intervenu au colloque « L'internet et le droit », le 26 septembre 2000 au Sénat.

La CNCIS a assisté à différents colloques et conférences :

Symposium mondial des technologies de l'information -25 février -2 mars 2000 – Poitiers

Eurosec 2000 -13-15 mars 2000 Paris

L'anonymat dans la société de l'information – fichage et démocratie – colloque de l'UJA 26 avril 2000 – Paris

Réunion du G8 -17-18 mai 2000 – Paris

17e salon professionnel de l'information électronique et de l'internet : – Donner un cadre juridique à la société de l'information – L'intelligence économique offensive -23-25 mai 2000 – Paris

Salon Interop -7,8,9 novembre 2000 – Paris

Les relations avec la presse sont assurées par le président ou par la déléguée générale.

Chapitre II

Le contrôle des autorisations

Les modalités du contrôle

Déroulement du contrôle

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

Le contrôle effectué par le président obéit, depuis la création de la Commission, à un rythme hebdomadaire, mais peut aussi s'exercer au jour le jour comme c'est le cas pour des demandes en urgence absolue.

La pratique du contrôle préalable à la décision d'autorisation suivie depuis plusieurs années, a permis de créer un dialogue avec les services demandeurs et la prise en compte à l'avance, par ces derniers, des éléments de la « jurisprudence » de la Commission grâce au relais 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 deux personnes désignées par celui-ci. 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 quantitatif

L'activité de contrôle comporte tout d'abord 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'interceptions octroyé aux trois ministères légalement 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. Les contingents réservés au ministère de la défense et à celui de l'intérieur, inchangés depuis 1997, se sont avérés cette année encore suffisants malgré l'accroissement de la consommation de télécommunications induite par la multiplicité des moyens à la disposition du public. Le seul secteur dans lequel une insuffisance est constatée est celui de la douane dont le quota d'interceptions est limité à 20. Un projet d'attribution de 20 interceptions supplémentaires a été soumis à la Commission en octobre 2000. Elle l'a approuvé.

La vérification, effectuée chaque semaine, du respect du nombre maximum d'interceptions simultanées a fait ressortir des encours moyens mensuels oscillant, au cours de l'année 2000, entre 1053 au plus bas et 1202 au plus haut, avec une moyenne annuelle de 1129 contre 1185 en 1999 (voir ci-dessous, chapitre III). Ces données montrent que l'augmentation du contingent, en 1997, de 1180 à 1540 pour faire face aux périodes de crise n'a pas provoqué d'augmentation brutale du nombre des demandes : leur volume est resté au niveau du quota antérieur à 1997.

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 formulation précise de ceux-ci permet une première appréciation des demandes. Les services doivent faire référence au motif légal. Ils doivent également justifier leur démarche par des explications circonstanciées et motivées. 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.

L'équilibre entre l'exigence de sécurité et la protection des libertés

Le contrôle s'attache d'une part à une identification aussi précise que possible des cibles, d'autre part à la fourniture d'informations quant à leur activité socio-professionnelle, afin de protéger les professions ou activités jugées sensibles en raison du rôle qu'elles jouent du point de vue des libertés fondamentales (presse, activités politiques ou syndicales, professions astreintes au secret professionnel).

Il importe aussi de s'assurer que le motif légal invoqué ne dissimule pas d'autres préoccupations que celle de la protection de la sécurité. 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. Il reste cependant que la loi de du 10 juillet 1991 étend sa protection sur tous de manière strictement égalitaire. Les informations complémentaires ainsi demandées ne constituent qu'un moyen de s'assurer du bien-fondé des motifs.

La « jurisprudence » de la CNCIS s'attache également à la protection des libertés de conscience et d'expression. Ainsi a-t-elle toujours estimé que le prosélytisme religieux, comme l'expression d'idéologies radicales, ne justifiaient pas en elles-mêmes la surveillance des correspondances téléphoniques. De même, les interceptions de sécurité ne sont pas destinées servir à la surveillance d'opposants de pays étrangers dès lors que la sécurité de la France n'est pas en danger ou que les autres objectifs mentionnés par la loi du 10 juillet 1991 ne sont pas en cause. En pratique, les demandes comme les autorisations sont très fortement orientées vers la prévention d'activités terroristes ou de criminalité organisée, souvent associées à des menaces concernant également la sécurité nationale, voire la sauvegarde du patrimoine économique et scientifique de la France. Le souci premier est la protection des personnes contre des activités terroristes ou mafieuses pouvant provoquer des violences ou des préjudices économiques ou financiers graves.

Le bilan du contrôle pour l'année 2000

Baisse des demandes

Sur le plan quantitatif tout d'abord, il faut observer une décrue importante des demandes d'interception initiales. Au nombre de 3044 en 1999, elles sont cette année 2756, soit 9,46 % de moins.

Faut-il y voir l'amplification du mouvement amorcé au deuxième semestre 1999 ? Ce chiffre nous ramène à la situation de 1995 après plusieurs années de hausse successives. Il est trop tôt pour en tirer des conclusions définitives, de même qu'il n'est pas possible d'affirmer qu'on observe, avec un décalage, le mouvement de fond qui affecte les interceptions judiciaires (en baisse de 43 % sur la période 95-99 : 11300 en 1995, 9336 en 1996, 9293 en 1997, 7919 en 1998, 6497 en 1999 ; les chiffres de 2000 ne sont pas encore communiqués). On peut se demander s'il faut y voir la conséquence de l'ouverture à la concurrence du secteur des télécommunications, se traduisant par des exigences financières plus grandes de la part des opérateurs, ou celle d'un moindre empressement de ceux-ci à respecter leurs obligations en matière de sécurité ; mais ce serait laisser de côté bien d'autres facteurs. Ainsi, il convient de souligner que la capacité d'interception dépend de l'évolution des techniques de communication et des coûts d'interception qu'elle induit, et qu'elle est étroitement liée aussi à la capacité d'exploitation, et par voie de conséquence, tributaire des effectifs affectés à cette tâche. On peut également faire observer une réalité nouvelle qui est l'augmentation de la consommation téléphonique liée à l'usage des portables : les échanges téléphoniques d'un usager y sont plus nombreux, même s'ils sont souvent plus brefs que sur le téléphone fixe. Cette évolution a pour effet direct d'alourdir le travail des « lecteurs » [1]. Enfin l'actualité peut entrer en ligne de compte. Il serait donc imprudent de tirer prématurément des conclusions de la baisse enregistrée en 2000.

Sur les 2756 demandes d'interceptions soumises au Premier ministre, 2689 ont été autorisées contre 2978 en 1999. Quelques-unes n'ont pu être réalisées pour des raisons techniques. Si l'on confronte ce chiffre (qui ne tient pas compte des renouvellements, mais ceux-ci correspondent à la poursuite d'écoutes existantes), ou celui des 1129 interceptions en cours en moyenne durant cette année, avec le nombre de lignes téléphoniques recensées sur le territoire national (33 998 000 à la fin du troisième trimestre 2000, plus 29 700 000 propriétaires de portables dénombrés fin décembre) force est de constater que, comme le souhaitait le législateur, l'interception de sécurité est une mesure dûment circonscrite.

Par ailleurs, le nombre des renouvellements continue de décroître depuis 1997 : 1803 en 1997, 1684 en 1998, 1599 en 1999 et enfin 1486 en 2000. Cette évolution traduit d'une part le travail mené au cours de ces années pour qu'une vigilance égale soit exercée sur les demandes de renouvellement et sur les demandes initiales, mais souligne d'autre part l'attention plus grande qui est portée aux facteurs qui justifient le renouvellement lui-même, en plus du motif légal d'interception. Les autorisations de renouvellement représentent cette année encore un peu plus du tiers des autorisations d'interception.

1) C'est à dire des agents qui transcrivent les interceptions.

Le nombre de demandes en urgence absolue est également en baisse. Depuis plusieurs années la CNCIS rappelait les principes qui devaient présider au recours à cette procédure : elle ne peut être justifiée que par la nécessité de répondre très vite à une situation imprévue ; cette nécessité doit être explicitée dans la demande ; une demande formulée tardivement pour faire face à un événement connu ou prévisible ne saurait justifier l'urgence absolue dès lors qu'elle peut être traitée en priorité selon la procédure normale ; l'urgence absolue ne doit pas être confondue avec l'importance de l'affaire et à l'inverse ne saurait absoudre une insuffisance de motif. (cf. rapport 1999 page13). 447 demandes de cette nature avaient été comptabilisées en 1998, 354 en 1999 et 197 en 2000, soit respectivement des pourcentages de 14,59 %, 11,62 % et 7,14 % par rapport aux demandes initiales. Il faut s'en réjouir pour deux raisons : d'une part cela signifie que l'actualité a été plus calme en termes de sécurité, d'autre part les observations précédemment formulées ont été suivies d'effet. Cette diminution des demandes en urgence absolue ne s'est pas traduite pas un report sur des demandes d'examen en urgence simple puisque les demandes de cette catégorie sont elles-mêmes passées de 514 en 1999 à 119 en 2000.

Constance dans la hiérarchie des motifs

Sur le plan qualitatif, l'ensemble des motifs légaux sont en baisse à l'exception de la prévention de la criminalité organisée (1256 demandes initiales contre 1145 l'an dernier, soit 45,57 %). En ce qui concerne les urgences absolues, le motif tiré de la prévention de la criminalité organisée devient également le plus fréquemment invoqué avec 103 cas sur 197, soit 52,28 %, alors que la prévention du terrorisme ne fonde cette année que 74 demandes en urgence absolue, soit 37,56 % des cas contre 73,72 % l'an dernier. La recherche de renseignements relatifs à la sauvegarde du potentiel scientifique et économique de la France ne représente plus qu'une part faible des demandes, particulièrement pour les deux dernières années. Globalement la masse des interceptions de sécurité est toujours répartie entre les différents fondements énoncés à l'article 3 de la loi suivant le classement décroissant observé de manière constante depuis maintenant six ans :
1 – prévention du terrorisme.
2 – prévention de la criminalité ou délinquance organisée ;
3 – sécurité nationale ;
4 – sauvegarde du potentiel économique et scientifique de la France.

Le dernier motif mentionné par la loi, relatif à la prévention de la reconstitution de groupements dissous, tombe en désuétude. La part des deux premiers motifs cités continue à représenter, cette année comme en 1999, 81 % des décisions initiales d'interception (80 % en 1998), et atteint 61 % des renouvellements accordés contre 56 % l'an dernier et 53 % en 1998. Ces constantes soulignent que de plus en plus les interceptions de sécurité privilégient la protection de la sécurité des personnes et sont moins orientées vers des préoccupations d'intérêt collectif. Ce mouvement, s'il se

confirme à l'avenir, ne fera que s'inscrire dans la ligne des préoccupations qui animent la plupart des États comparables.

Certains des fondements légaux d'interception suscitent traditionnellement davantage de demandes de renouvellement que d'autres. C'est ainsi que les demandes relatives à la prévention du terrorisme fondent 50 % des prolongations et la sécurité nationale 37 %, la part du premier de ces motifs croissant de manière constante depuis plusieurs années.

Bilan des observations

276 demandes (151 demandes initiales et 125 demandes de renouvellement) ont, cette année, donné lieu à observations : c'est le même pourcentage que l'an dernier. Il s'agit généralement de demandes qui méritent quelques précisions ou explications complémentaires, ou bien dont l'objectif ne paraît pas suffisamment justifié sur le fond.

114 refus de la demande ou retraits par les services (67 pour les demandes initiales et 47 pour les renouvellements) ont fait suite à ces observations, qu'il s'agisse d'appréciations négatives ou simplement de réserves ; 4 interceptions ont été interrompues parce qu'elles n'apparaissaient plus nécessaires. Dans 52 cas, l'examen des demandes a conduit à solliciter des renseignements complémentaires, qui ont permis la formulation d'un avis positif. 32 interceptions ont été autorisées sous réserve d'un contrôle de la « production », c'est-à-dire des transcriptions d'écoutes. Enfin à 54 reprises a été recommandée une limitation à une durée inférieure à 4 mois, ou l'exclusion d'un renouvellement. Enfin le signalement de doublons – demandes simultanées présentées par des services différents sur un même objectif – a conduit dans quelques cas à un refus destiné à prévenir des risques d'investigations concurrentes.

Cette année encore les avis négatifs du président et les réserves ou observations de la Commission ont été suivis sans exception. Dans quelques cas le délégué du Premier ministre a décidé un refus alors que les observations du président n'avaient pas conduit ce dernier à exprimer un avis entièrement négatif mais à suggérer des restrictions.

Enfin d'une manière générale, les lignes directrices définies dans les différents rapports d'activité et notamment celui de 1999 ont été suivies de manière tout à fait satisfaisante par les différents ministères en ce qui concerne la présentation de leurs demandes d'interception.

Chapitre III

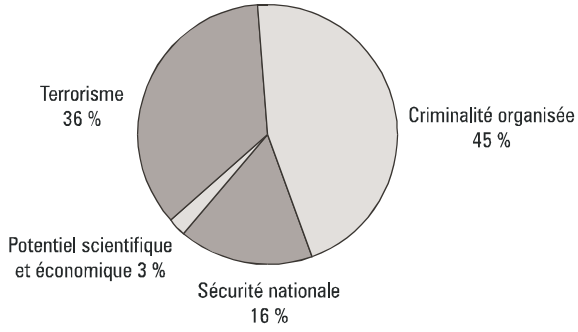
Les statistiques

Les demandes de construction

État des demandes d'interception initiales de l'année 2000

Mois	Demandes initiales de constructions	Dont urgence absolue	Accordées
Janvier	244	20	243
Février	289	18	283
Mars	238	14	234
Avril	253	19	247
Mai	218	15	205
Juin	245	21	237
Juillet	218	8	216
Août	169	20	159
Septembre	163	11	159
Octobre	275	21	274
Novembre	228	17	226
Décembre	216	13	206
Totaux	**2 756**	**197**	**2 689**

Répartition des motifs

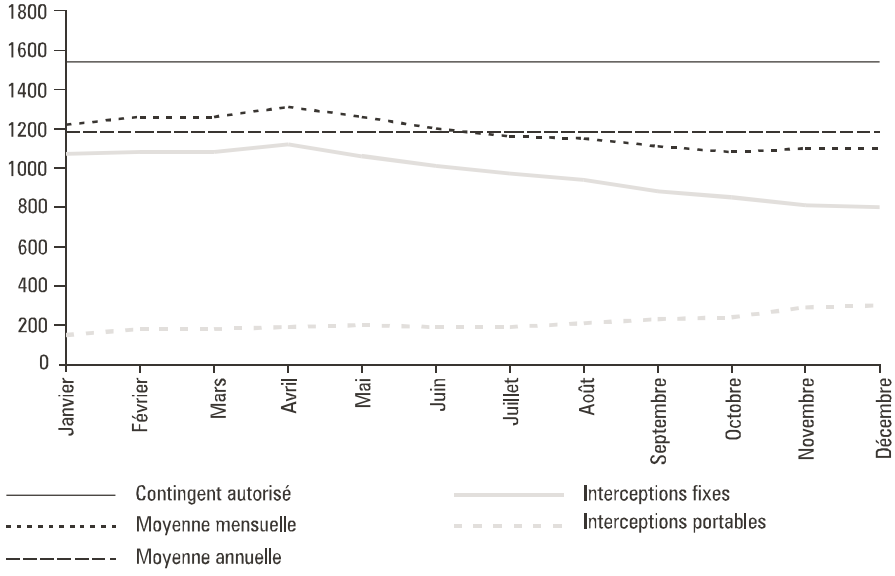


État comparatif sur cinq ans

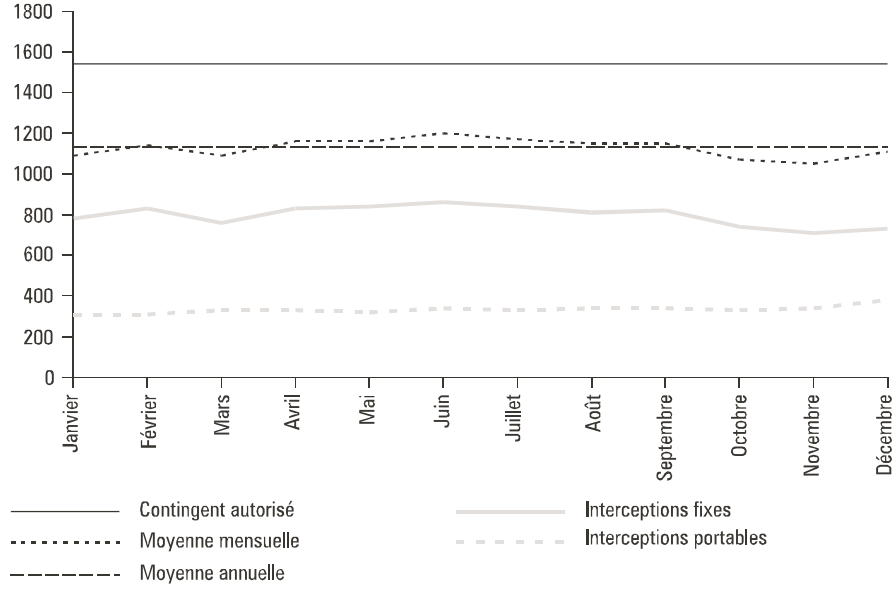
Motifs	1996	1997	1998	1999	2000
Sécurité nationale	497	465	491	495	449
Potentiel scientifique et économique	125	175	120	87	72
Terrorisme	1 039	1 190	1 327	1 317	979
Criminalité organisée	1 123	1 073	1 124	1 145	1 256
Groupements dissous	20	7	0	0	0
Totaux	**2 804**	**2 910**	**3 062**	**3 044**	**2 756**

L'utilisation du contingent global d'interceptions

Moyennes mensuelles et annuelle 1999



Moyennes mensuelles et annuelle 2000



Les renouvellements d'interception

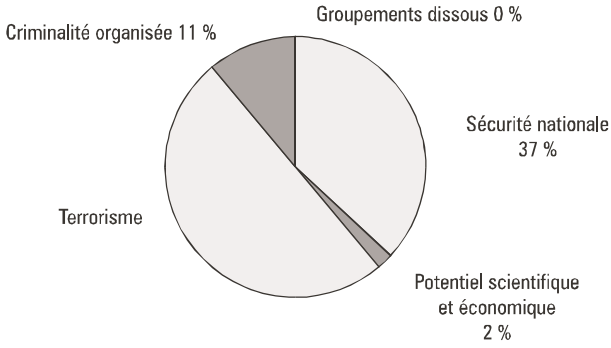
État des renouvellements pour l'année 2000

Mois	Demandes de renouvellements	Renouvellements
Janvier	109	108
Février	83	80
Mars	128	120
Avril	121	118
Mai	142	140
Juin	162	159
Juillet	156	153
Août	156	151
Septembre	101	98
Octobre	120	113
Novembre	140	136
Décembre	115	110
Totaux	**1 533**	**1 486**

Répartition des motifs

Année 2000

Sécurité nationale	Potentiel scientifique et économique	Terrorisme	Criminalité organisée	Groupements dissous
551	27	744	163	1

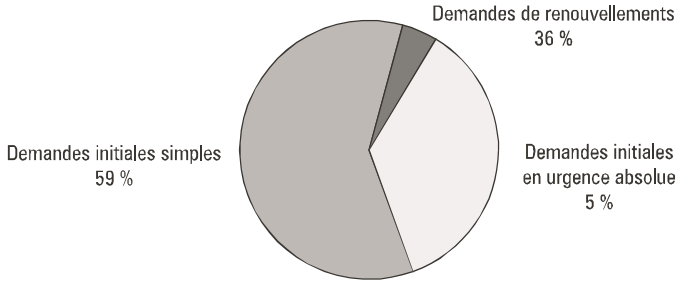


État comparatif sur cinq ans

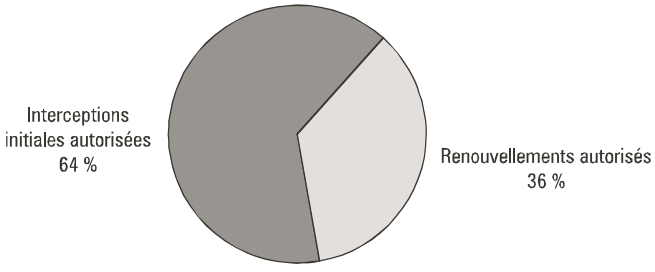
Motifs	1996	1997	1998	1999	2000
Sécurité nationale	744	779	665	597	551
Potentiel scientifique et économique	138	141	118	99	27
Terrorisme	717	721	693	719	744
Criminalité organisée	197	155	199	181	163
Groupements dissous	23	7	9	3	1
Totaux	**1 819**	**1 803**	**1 684**	**1 599**	**1 486**

Activité de la CNCIS : demandes initiales et renouvellements

Répartition des demandes entre interceptions et renouvellements d'interception



Répartition entre autorisations d'interception et autorisations de renouvellements



Le contrôle de l'exécution

Enregistrement – Transcription

Les visites opérées sur sites par la CNCIS permettent de rappeler les principes et la vigilance qui s'imposent en ces matières.

Sur le premier point, la mise en place progressive d'une nouvelle technologie, permettant l'effacement automatique de l'enregistrement au plus tard à l'expiration du délai de 10 jours prévu par l'article 9 de la loi, devrait apporter un gain de temps appréciable pour les agents chargés de l'exploitation. Le registre normalisé mis précédemment en place pour faciliter le contrôle devra être revu pour tenir compte de cette technologie.

Lorsque la cryptologie se sera davantage répandue, les contraintes du déchiffrement préalable poseront le problème des conditions de mise en œuvre de ce délai.

Quant aux transcriptions, selon l'article 12 de la loi du 10 juillet 1991, elles doivent être détruites dès que leur conservation n'est plus indispensable à la réalisation des fins mentionnées à l'article 3. Or peu d'entre elles méritent d'être conservées durablement. Un suivi périodique devrait permettre d'éliminer les documents qui ont perdu leur actualité. Cela suppose de lutter contre une tendance naturelle qui, en l'absence d'instruction contraire, porte à la conservation de ces documents. Peu à peu l'habitude inverse doit s'installer, d'autant qu'elle répondrait aussi à l'exigence d'efficacité en obligeant à une meilleure connaissance des transcriptions conservées. Depuis la mise en place, en 1996, du système centralisé de contrôle des destructions pour la région parisienne, les transcriptions conservées au-delà du délai de quatre mois sont devenues résiduelles. Malgré quelques appréhensions initiales, il n'en est pas résulté de difficulté de fonctionnement particulière pour les services. La réalité est un peu plus dispa-

rate en province où cependant un effort d'apurement se fait jour progressivement sous la responsabilité des chefs de services, parfois avec des délais plus rigoureux que celui préconisé en 1996.

La durée des interceptions

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 4 mois par renouvellement de l'autorisation avant l'expiration de la période en cours.

Une étude faite à partir des interceptions ayant pris fin pendant l'année 2000 fait ressortir une durée moyenne d'interception de 4 mois contre 5 mois 5 jours en 1999.

À l'analyse, il apparaît que 42 % des renouvellements autorisés en 2000 constituent des premiers renouvellements. Si on prend en considération ceux qui prolongent des interceptions initiales autorisées en 1999 et 2000 on observe qu'ils représentent 73,37 % de l'ensemble de ces mesures. Ces pourcentages sont pratiquement identiques à ceux relevés l'année dernière tant en ce qui concerne les premiers renouvellements que ceux faisant suite à des écoutes initiales enregistrées au cours des deux années 1998 et 1999. Cette anné, les interceptions initiales de 1997 et de 1998 sont à l'origine de 13,41 % des renouvellements autorisés et celles des années antérieures de 13,22 %.

Une comparaison effectuée avec l'état de l'année 1999 fait ressortir que le volume de ces mesures s'érode avec le temps. Ainsi en 1999, les interceptions initiales autorisées en 1998 et 1999, celles initiées en 1996 et 1997 et enfin les interceptions antérieures étaient à l'origine de respectivement 73,3 %, 14,3 % et 12,3 % des renouvellements. En 2000, seulement 46 %, 7,3 % et 8,9 % d'entre eux correspondent encore à des écoutes autorisées au cours des mêmes périodes de référence.

Enfin 518 constructions ont été supprimées d'office à l'expiration de la période de 4 mois en l'absence de toute manifestation de volonté de la part des services concernés. Ce phénomène peut être pour partie imputable au fait, déjà signalé dans le précédent rapport, que les services négligent parfois de demander la suppression de l'interception alors même qu'ils ont cessé de l'exploiter, laissant au GIC le soin de la supprimer d'office à l'échéance des quatre mois.

Le contrôle du GIC

L'exigence d'un contrôle efficace se traduit par des efforts menés dans deux directions : d'une part la création et l'équipement d'antennes régionales, destinées à asseoir le contrôle sur une base géographique plus proche et à permettre une appréhension plus rigoureuse de l'activité d'interception hors de la région parisienne, d'autre part la modernisation du GIC pour lui donner la capacité technique d'une meilleure centralisation de l'exécution.

Les antennes régionales PACA, Rhône-Alpes et Sud-Ouest, désormais en place, sont un facteur important de rationalité et de sécurité, et un instrument très précieux d'amélioration du contrôle central. L'objectif n'est pas d'augmenter la capacité d'interception mais d'améliorer les pratiques et de moderniser les techniques et les conditions matérielles des installations dans la double perspective d'une rigoureuse application de la loi du 10 juillet 1991 et d'une meilleure protection du secret-défense.

Les moyens utilisés à cette fin sont de deux ordres :
– moyens matériels permettant un regroupement des implantations, un meilleur emploi des personnels par l'économie réalisée sur des temps de transport ou des tâches de manutention, la prise en compte dans la conception même des matériels des exigences de la loi (délai d'enregistrements, contrôle des transcriptions, amélioration de la centralisation de l'exploitation) ;
– moyens humains, d'autre part, grâce à une meilleure organisation des tâches : le relais local assuré par les antennes régionales, la liaison permanente avec les services utilisateurs permettent une transmission directe et un rappel constant des directives procédurales et des pratiques mises en œuvre par le GIC central, ainsi que des recommandations ou observations du président de la commission de contrôle.

Ces antennes sont à même d'exercer un contrôle renforcé sur l'activité régionale de même nature que celui exercé par le siège du Groupement interministériel de contrôle sur l'activité de sa propre zone d'intervention directe. À terme les efforts menés devraient permettre de réduire émiettement et dispersion et conduire à la disparition de sites trop petits.

Parallèlement, la modernisation technique du GIC se poursuit. Elle tend à permettre à la fois un traitement direct et une amélioration qualitative et quantitative notable de la capacité de contrôle du GIC central. La part de l'activité directement soumise au contrôle de celui-ci a progressé de manière continue au cours des deux dernières années.

Cet effort de structuration et de clarification répond à l'objectif de centralisation posé par l'article 4 de la loi du 10 juillet 1991. Il est aussi de nature à faciliter la tâche de l'autorité de contrôle et lui permet de vérifier que non seulement la procédure, mais l'esprit de la loi, c'est-à-dire l'équilibre entre la protection des libertés et l'exigence de sécurité, sont respectés.

Service administratif du Premier ministre, le GIC est un élément clé du système de contrôle instauré par la loi du 10 juillet 1991. La comparaison avec l'étranger fait ressortir les avantages qu'offre la centralisation pratiquée en France pour l'exercice du contrôle incombant à la CNCIS. Enfin ce contrôle externe fait probablement du GIC un des services administratifs dont le fonctionnement et l'activité sont les plus précisément décrits.

Ces caractéristiques justifieraient qu'il soit doté d'un véritable statut administratif, qui lui fait actuellement défaut.

Chapitre V

Les visites sur le terrain

La CNCIS a développé cette année son action sur le terrain et a considérablement accru le nombre de ses déplacements. Les objectifs sont les différents services utilisateurs d'interceptions, les installations, les services spécialisés des opérateurs de télécommunications, ainsi que le cas échéant les fabricants de matériels soumis à autorisation.

Objectifs et méthodes

Ces visites se font soit à l'improviste, ce qui a été le cas à l'occasion de deux tournées organisées en juillet et septembre dans la périphérie parisienne et dans l'Est – le contrôle porte alors principalement sur les interceptions en cours – soit avec quelques jours de préavis, lorsqu'il s'agit d'examiner le fonctionnement administratif, l'organisation mise en place par les services pour assurer les interceptions de sécurité et de vérifier le respect des dispositions de la loi du 10 juillet 1991.

Les visites peuvent revêtir un aspect formel à l'occasion de l'inauguration de locaux ou d'antennes, ou de l'implantation de nouveaux matériels. Elles prennent un caractère plus systématique et plus approfondi lorsque les réalités locales sont une donnée importante de l'activité d'interception, comme cela a été le cas pour un déplacement en Martinique et en Guadeloupe.

Ces déplacements peuvent être effectués par les membres de la Commission elle-même, par la déléguée générale ou par le chargé de mission.

Au total ont été visités, sous l'une ou l'autre forme, le Sud-ouest, la Bretagne, la région PACA, la région Centre, la périphérie parisienne, l'Est et

deux départements d'Outre-mer. Vingt-cinq sites ont pu être ainsi contrôlés.

La CNCIS s'est rendue à cinq reprises dans les services d'opérateurs de télécommunications et une douzaine de rencontres ont été tenues avec leurs agents ou représentants.

Ces déplacements ont porté enfin sur deux entreprises de commercialisation ou fabrication de matériels soumis à autorisation.

Dans tous les cas, les représentants de la CNCIS dressent un inventaire des pratiques et procédures mises en œuvre pour l'application de la loi du 10 juillet 1991, apportent des éclaircissements et informations sur des points qui peuvent être mal connus, expliquent et font connaître le rôle de la CNCIS, recueillent des observations auprès des personnels rencontrés. Vis-à-vis des opérateurs, c'est l'occasion d'évoquer les problèmes techniques mais surtout les deux types d'obligations qui pèsent sur eux : celle de coopérer à la réalisation des interceptions de sécurité conformément à l'article 22 de la loi du 10 juillet 1991 et aux articles L 35-6 et D 98-1 du code des télécommunications, et d'autre part celle de protéger la confidentialité de ces opérations en prenant les mesures de sécurité indispensables tant sur le plan des locaux que sur celui des personnels ou sur les procédures. Les contacts avec le secteur de la fabrication et de la commercialisation de matériels visés par l'article 226-3 du code pénal sont l'occasion de sensibiliser, entre autres, les professionnels aux exigences de la tenue du registre des mouvements instauré par l'arrêté du 15 janvier 1998 en application de l'article R. 226-10 du code pénal.

Bilan

Les antennes du GIC sont des facteurs d'amélioration technique et des éléments de centralisation de nature à favoriser la rationalité et la systématisation du contrôle. Leur inauguration a parfois permis de discerner quelques tensions de la part de certains services, voire des réticences devant l'obligation de passer par des centres spécialisés dont ils redoutent qu'ils restreignent leur liberté de manœuvre. Ainsi, malgré quarante ans d'existence du GIC et presque dix ans d'application de la loi du 10 juillet 1991, la centralisation continue à susciter quelques résistances qui s'estompent cependant assez vite.

Les visites destinées à vérifier sur place la nature des procédures mises en place avec les opérateurs ont fait apparaître qu'un réel effort sur les mesures de sécurité avait été mené postérieurement au cambriolage intervenu dans les locaux de France Télécom Mobile au printemps 2000. Cet effort doit être maintenu. Les initiatives, prises dans certains secteurs géographiques, de procéder à une destruction sous contrôle « GIC » des « cartons » devenus sans objet paraissent porter leurs fruits. Ce procédé peut engendrer cependant un léger différé de la destruction. La présence du

GIC à ce stade a également pour avantage de rappeler les opérateurs à leurs obligations en matière d'interceptions de sécurité et la rigueur qui s'impose en ce domaine.

Les visites de services ou les contrôles impromptus menés en différents sites ont enfin permis de rappeler, à l'occasion, quelques points sur le traitement des transcriptions, l'usage exclusif du matériel de dotation, la vigilance à observer quant aux demandes de cessation d'interception et à leur exécution, la sécurité des locaux etc. Ces visites n'ont pas amené la découverte de dysfonctionnements significatifs. L'accueil réservé par les personnels en charge de cette activité s'est avéré tout à fait positif.

Le bilan des déplacements impromptus, plus directement orientés vers un objectif de contrôle, est satisfaisant : les règles de fond fixées par la loi du 10 juillet 1991 sont connues et correctement appliquées ; la stabilité de personnels expérimentés, notamment en province, est un facteur de rigueur et de sécurité et assure la transmission de pratiques, qui ne sont pas véritablement « codifiées » et pour lesquelles une marge relativement importante est laissée aux services locaux. Cette situation fait apparaître dans certains secteurs un besoin d'information sur les modes opératoires à respecter et un souci d'être mieux informé des usages. Ces visites peuvent donner l'occasion de resserrer les liens avec l'instance centrale et permettre quelques ajustements fonctionnels.

Les efforts de modernisation en cours peuvent conduire par ailleurs à adopter une nouvelle répartition des tâches qui tend à séparer le travail d'exploitation de l'interception et l'investigation sur le terrain.

Le déplacement aux Antilles a permis de constater que les réalités économiques et sociales sont très différentes dans les trois îles visitées – Guadeloupe, Saint-Martin, Martinique – mais que ces différences sont sans incidence sur l'activité d'interception.

Les deux départements français des Antilles apparaissent comme des îlots de prospérité dans la région caraïbe.

La Guadeloupe est cependant le département où la situation est la plus difficile : agitation syndicale permanente préjudiciable notamment au tourisme et aux investissements, consommation de crack en augmentation, montée de la délinquance violente, chômage important.

L'accroissement de la délinquance violente existe également en Martinique, mais à un degré moindre. Cette île, en revanche, subit moins de tensions politiques ou syndicales. Saint-Martin enfin, sous-préfecture de la région Guadeloupe, ne montre pas d'affinités particulières avec le chef-lieu. Sa division entre les Pays-Bas et la France, l'absence de frontière matérialisée, l'unicité de la population répartie sur l'ensemble de l'île, l'immigration très importante, la difficulté de faire appliquer la loi malgré une forte présence des services de sécurité, contribuent à faire de cette sous-préfecture, où la langue naturelle est l'anglais, un territoire atypique.

Sur le plan des télécommunications, les portables et l'internet connaissent, aux Antilles comme ailleurs, un succès toujours grandissant. Saint-Martin présente en outre la particularité de voir prospérer sur son sol, notamment dans la partie hollandaise, des opérateurs multiples et des normes téléphoniques diverses.

Les installations « GIC » dans ces départements sont satisfaisantes et bien tenues. Des économies ont été réalisées par la limitation des déplacements des personnels. Les procédures sont respectées. L'activité en revanche est faible depuis quelques années. En effet, les îles offrent sans doute des motifs d'interceptions judiciaires, mais peu de motifs d'interceptions de sécurité ; elles ne connaissent pas actuellement de phénomène terroriste et peu de criminalité véritablement organisée.

Chapitre VI

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 quarante-cinq réclamations de particuliers. Huit constituaient des demandes de renseignements sur la législation, les autres ont 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. Le cadre de l'intervention de l'autorité de contrôle paraît avoir été mieux compris et il n'y a pas eu lieu de signaler de difficultés particulières en ce domaine. Il faut préciser que nombre de requérants s'adressent à la CNCIS téléphoniquement avant toute démarche écrite. Ce contact préalable permet de prévenir des démarches inappropriées lorsqu'il s'agit notamment d'appels malveillants, de problèmes relevant de la saisine de l'autorité judiciaire (soupçons d'écoutes illégales à caractère privé) ou enfin de dysfonctionnements techniques classiques ; il permet aussi de réorienter les demandeurs vers les services compétents.

Il convient de souligner la décision rendue pour la première fois par le Conseil d'État cette année sur l'étendue des pouvoirs exercés sur le fondement de l'article 15 de la loi en vertu duquel « 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 ». Saisi en 1999

d'une demande d'annulation pour excès de pouvoir par un réclamant, le Conseil d'État a rendu le 28 juillet 2000 un arrêt rejetant la requête dirigée contre une lettre du président de la CNCIS en date du 1er décembre 1999 par laquelle celui-ci informait le réclamant qu'il ne pouvait être donné suite à sa demande d'enquête.

L'intéressé refusait d'indiquer la ou les lignes téléphoniques susceptibles d'être concernées. Sans alléguer l'existence d'une interception dont il aurait pu être lui-même l'objet, il demandait à la Commission de vérifier si la surveillance policière qu'il pensait avoir décelée ne s'expliquait pas par une interception de sécurité sur la ligne d'une personne qui restait à déterminer.

Il lui avait été répondu que la Commission n'avait pas le pouvoir d'enquêter sur les moyens par lesquels les services de sécurité avaient pu obtenir un renseignement, sa mission se limitant à contrôler si une interception était effectuée conformément à la loi.

La réponse du Conseil d'État a été la suivante :

... Sur la compétence du Conseil d'État :

Considérant qu'aux termes de l'article 2 du décret susvisé du 30 septembre 1953 : « Le Conseil d'État reste compétent pour connaître en premier et dernier ressort :... 6° Des recours en annulation dirigés contre les décisions administratives des organismes collégiaux à compétence nationale » ; que la commission nationale de contrôle des interceptions de sécurité, instituée par l'article 13 de la loi du 10 juillet 1991 susvisée, est un organisme collégial à compétence nationale ; que le Conseil d'État est par suite compétent pour connaître en premier ressort de la demande d'annulation de la décision signée par le président de la commission, au nom de cette dernière, et prise dans l'exercice de la compétence que cette commission tient de l'article 15 de la loi du 10 juillet 1991 susvisée ;

Sur la légalité de la décision attaquée :

Sans qu'il soit besoin de statuer sur la fin de non recevoir opposée à la requête :

Considérant qu'aux termes de l'article 15 de la loi du 10 juillet 1991 susvisée : « 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 » ;

Considérant que M. D., soupçonnant l'existence d'écoutes téléphoniques opérées sur les lignes téléphoniques de ses relations, qui selon lui auraient été établies pour les besoins d'une opération de police, a saisi de ces faits le président de la commission nationale de contrôle des interceptions de sécurité, en se refusant toutefois à fournir à cette autorité les numéros de lignes téléphoniques ayant selon lui fait l'objet de ces écoutes ; qu'en refusant de donner suite à cette saisine, qui, dans les conditions dans lesquelles

elle était faite, tendait à ce que la commission effectue une enquête auprès des services de police aux fins de rechercher l'origine des informations qui avaient déclenché leur action, et non à ce qu'elle effectue sur des lignes téléphoniques identifiées les contrôles que la loi lui a donné pour mission d'opérer, le président de cette commission n'a pas méconnu la portée de la loi ; qu'il suit de là que M. D. n'est pas fondé à demander l'annulation de la décision attaquée ;

DÉCIDE :

Article 1er : La requête de M. D. est rejetée.

Article 2 : (notification).

Les avis à l'autorité judiciaire

La CNCIS n'a pas eu à user des dispositions du 2ème 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 elle est exonérée du respect du secret-défense qui pèse sur la matière.

Cette disposition a été introduite par un amendement parlementaire présenté par la commission des lois de l'Assemblée nationale. Celle-ci avait jugé utile d'expliciter dans la loi du 10 juillet 1991 l'obligation qui résulte de l'article 40 alinéa 2 du code de procédure pénale, en en précisant notamment le cadre.

La disposition de l'article 17, alinéa 2 est tout à fait comparable à celle énoncée dans l'article 21, 4ème 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. »

Rappelons qu'aux termes de l'article 40 du code de procédure pénale « toute autorité constituée ou officier public ou fonctionnaire qui dans l'exercice de ses fonctions acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs ».

Dans un arrêt du 27 octobre 1999, le Conseil d'État a été amené à préciser les conditions dans lesquelles cette obligation s'exerçait pour la CNIL. Selon les termes de cet arrêt... « il appartient à la CNIL d'aviser le procureur de la République des faits dont elle a connaissance dans l'exercice de ses at-

tributions si ces faits lui paraissent suffisamment établis et si elle estime qu'ils portent une atteinte suffisamment caractérisée aux dispositions dont elle a pour mission d'assurer l'application ».

Il en ressort que le Conseil d'État a fait une application combinée du texte spécifique de la loi du 6 janvier 1978 et de l'article 40 du code de procédure pénale pour définir le cadre juridique de l'obligation qui pèse sur l'autorité administrative et la marge d'appréciation dont elle dispose.

Le devoir de dénonciation ne se traduit pas pour elle par une obligation de transmission mécanique au parquet, mais lui laisse un pouvoir d'appréciation quant aux faits, qui doivent lui paraître suffisamment établis, et quant à l'atteinte à la loi, dont il lui appartient d'estimer si elle est suffisamment caractérisée. Cette marge d'appréciation s'exerce sous le contrôle du juge administratif.

La solution ainsi dégagée, qui exprime la complémentarité de l'activité de cette autorité administrative indépendante et de l'activité judiciaire en matière d'infraction pénale, intéresse l'ensemble des autorités administratives et paraît totalement transposable à la CNCIS. Elle doit être appréciée en tenant compte d'une autre jurisprudence, selon laquelle le juge administratif se déclare incompétent pour connaître des décisions positives de saisine de l'autorité judiciaire, considérées comme inséparables de la procédure judiciaire : c'est alors au juge judiciaire qu'il appartient de dire si l'infraction est ou non caractérisée.

Pour sa part, la Cour de cassation, dans un arrêt du 3 février 1998, a précisé, que l'exercice du signalement prévu par la loi, dans une espèce qui concernait là encore la CNIL, ne constituait pas une dénonciation calomnieuse même si les faits dénoncés n'avaient pas conduit finalement à la condamnation du prévenu.

Chapitre VII

Le contrôle du matériel

Outre les missions qui lui sont propres, la CNCIS fait partie de la commission consultative instituée auprès du Premier ministre par l'article R. 226-2 du code pénal. Cette commission examine les dossiers présentés en vue de la fabrication, l'importation, l'exposition, l'offre, la location, la vente, l'acquisition ou la détention de deux types de matériels : ceux conçus pour réaliser les opérations pouvant constituer les délits d'interception ou de détournement des correspondances émises, transmises ou reçues par la voie des télécommunications (art. 226-15 alinéa 2 du code pénal) et ceux qui, conçus pour la détection à distance des conversations, permettent de réaliser l'infraction d'atteinte à la vie privée (art. 226-1 du même code). Les autorisations sont ensuite délivrées par le Premier ministre ; en fait et par délégation, par le secrétaire général de la défense nationale.

La CNCIS a toujours considéré qu'un véritable contrôle des interceptions de sécurité devait porter non seulement sur les documents et moyens mis en œuvre par les services de l'État conformément à la loi de 1991, mais également sur les matériels permettant de contourner la loi. À cette fin, ses représentants ont rencontré différents professionnels de la fabrication et de la commercialisation de ces matériels et ont visité leurs établissements. On rappellera que depuis sa création la CNCIS a dénoncé les insuffisances du contrôle opéré sur ces matériels. Elle a participé activement à la création de

la commission consultative [1] qui a été installée le 11 septembre 1997 en application du décret 97-757 du 10 juillet 1997.

Présentation du dispositif

Depuis lors l'activité de celle-ci ne cesse de croître. Le nombre de dossiers examinés est passé de 240, en 1998 à 456, en 1999, pour atteindre 625, en 2000, soit une progression en un an de 37 % et de 160 % depuis la réforme de 1997.

Les demandes se répartissent en deux grandes catégories dites, par simplification, de commercialisation et de détention. Les premières tendent à obtenir l'autorisation mentionnée à l'article R. 226-3 du code de procédure pénale (fabrication, importation, exposition, offre, location ou vente des matériels concernés) ; les secondes visent l'acquisition ou la détention (art. R. 226-7 du même code).

En proportion, les demandes d'autorisation de détention ont représenté en 2000 environ 86 % du total. Le secteur privé est de loin, à concurrence d'environ 85 %, le principal demandeur. Ces chiffres ne rendent compte que de façon grossière du nombre d'appareils réellement en cause. En effet, les fabricants, par exemple, se voient délivrer des autorisations par type de matériels et non par unité. De la même façon, s'agissant cette fois de la détention, une entreprise qui a besoin de 10 appareils identiques pour des raisons de mesure ou de maintenance ne déposera qu'une demande et ne recevra qu'une autorisation valable pour les 10 appareils.

À quelques rares exceptions près, le nombre le plus fiable est celui des enregistreurs de communications téléphoniques car chaque demande ne porte que sur un appareil. Il est de 240 pour l'année 2000. C'est ici aussi le secteur privé qui est le plus grand demandeur avec environ 82 % des demandes.

Ce sont finalement 1163 autorisations qui ont été délivrées en 2000, toutes catégories de demandes et de matériels confondues.

Pour compléter ce dispositif, un registre uniforme retraçant les opérations relatives à ces matériels a été mis en place par arrêté du 15 janvier

1) La commission consultative est composée comme suit :
– 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 ;

1998. En effet, toute personne morale ou physique qui les commercialise doit être titulaire d'une autorisation et doit consigner sur son registre les références de l'autorisation de ses clients. Il est ainsi possible de reconstituer la chaîne des différents possesseurs de matériels et éventuellement de constater les défaillances. Celles-ci sont susceptibles de constituer le délit prévu par l'article 226-3 du code pénal et puni d'un emprisonnement d'un an et d'une amende de 300 000 francs. L'absence de tenue de ce registre est elle-même une infraction sanctionnée par une amende de 3 000 francs. À ce propos, la CNCIS déplore de nouveau cette année que le projet de loi renforçant la lutte contre les écoutes sauvages déposé au Sénat en mars 1997, et notamment la dotant de pouvoirs de contrôle de ces registres, n'ait pas été encore inscrit à l'ordre du jour.

Un souci constant d'amélioration

L'expérience de trois années a permis à la commission consultative d'affiner sa doctrine afin d'améliorer la gestion des matériels soumis à autorisation. L'objectif est, à terme, de simplifier le traitement des matériels dont la nature et l'usage les rendent a priori peu dangereux du point de vue des atteintes à la vie privée, et de concentrer les efforts sur le suivi des matériels « sensibles ».

La commission consultative a ainsi décidé, par exemple, que l'autorisation de commercialisation induisait le droit pour ses titulaires de détenir le matériel concerné sans qu'ils aient à solliciter une autorisation de détention. De la même façon, l'exigence d'une description précise de l'utilisation envisagée permet une meilleure compréhension des demandes et en facilite l'examen.

Le SIMTEC (Syndicat de l'Instrumentation de Mesure, du Test, de l'Énergie et des Communications dans le domaine de l'électronique) a souhaité apporter sa contribution à la réflexion sur la mise en place d'un système qui, d'une part, garantisse l'application stricte des textes pour les appareils conçus pour l'interception ou l'écoute avec ou sans enregistrement, et qui, d'autre part, n'entrave pas le commerce ou l'usage de matériels à vocation industrielle tels les appareils de mesure ou de test.

Cette collaboration entre instances privée et publique devrait permettre de surmonter les difficultés de classement de certains matériels. Ces difficultés sont liées à la technologie ou au caractère dual de certains d'entre eux, indispensables à certaines activités professionnelles et pouvant permettre par ailleurs la commission d'infractions pénales. Une meilleure information des professionnels leur permettrait de mieux formuler leurs demandes et de les voir traitées plus rapidement.

La question spécifique des enregistreurs

En matière d'enregistreurs de conversations, ce sont aujourd'hui, après les établissements financiers, les sociétés de télésurveillance et les services d'urgence, des domaines d'activité de plus en plus variés qui sont concernés : entreprises de logistique, sociétés de taxis, vente par correspondance, société de production de jeux télévisés... Certaines demandes ne viennent en fait que régulariser des situations existantes.

Le motif des demandes est, dans la grande majorité des cas, de se prémunir contre tout litige en se constituant un élément de preuve, ou d'avoir la possibilité de réécouter un appel pour organiser une intervention ou des secours, ou encore de vérifier le comportement au téléphone des agents au contact de la clientèle.

Soucieux d'éviter les dérapages et usages abusifs des enregistrements, la commission consultative et le secrétariat général de la défense nationale (SGDN) rappellent aux bénéficiaires d'autorisations le cadre dans lequel la détention est autorisée : respect de l'usage indiqué dans la demande, information des appelants du fait qu'ils sont enregistrés, information des représentants des salariés de la mise en place du dispositif.

À ces fins, il est demandé une déclaration d'engagement rédigée par le demandeur. En outre, les autorisations comportent les mentions suivantes :
– « Ce matériel ne peut être mis en œuvre par le titulaire que pour le seul usage spécifié dans le dossier auquel correspond l'autorisation qui lui est délivrée » ;
– « Le secret des correspondances émises par la voie des télécommunications et l'intimité de la vie privée sont garantis par la loi. Y porter atteinte peut être constitutif de l'infraction prévue à l'article 226 du code pénal ».

Ainsi, le rapprochement de la demande et de l'autorisation définit clairement le champ de la responsabilité (notamment pénale) du demandeur.

De plus, suivant en cela l'avis de la CNCIS, la commission consultative et le SGDN usent de la faculté offerte par l'article R. 226-9 du code de procédure pénale de subordonner l'utilisation des appareils à certaines conditions.

Ainsi, a-t-il été estimé qu'une vigilance particulière s'imposait quant au délai de conservation des enregistrements des conversations téléphoniques afin de limiter les risques d'abus. La quasi totalité des demandeurs s'engagent sur des délais allant de quelques jours à deux mois. Ces délais permettent de traiter les demandes téléphoniques de la clientèle, de ré-écouter le cas échéant les messages d'alerte ou de détresse, d'exploiter l'enregistrement par exemple à des fins pédagogiques, de conserver une trace le temps de la formalisation ou de la confirmation d'un acte ou d'un contrat. Dans la pratique, pour un délai supérieur à deux mois il est demandé aux intéressés de justifier d'une contrainte prévue par un texte.

Deux sociétés ont saisi le tribunal administratif de Paris de la question du délai qui leur est imposé. Les procédures sont actuellement en cours.

Il convient de relever que les règles ou les contraintes particulières parfois invoquées pour justifier des demandes de délais de conservation des enregistrements pouvant aller jusqu'à trente ans doivent être remises à leur juste place dans la hiérarchie des normes. La position que la CNCIS n'a de cesse de défendre est que les libertés individuelles ne doivent en aucun cas être sacrifiées aux lois du marché. Des contacts ont d'ailleurs été pris avec le secrétaire général de la Commission nationale de l'informatique et des libertés pour tenter de coordonner l'action des différentes autorités publiques en la matière.

Un contentieux rare

En 2000, l'examen de l'ensemble des dossiers a conduit à proposer au Premier ministre, qui a suivi ces avis, de prononcer 9 refus et 5 retraits. Rappelons que les retraits peuvent être prononcés dans quatre cas limitativement prévus par l'article R. 226-11 du code pénal :
– fausse déclaration ou faux renseignement ;
– modification des circonstances au vu desquelles l'autorisation a été délivrée ;
– non-respect par le bénéficiaire de l'autorisation des dispositions réglementaires ou des obligations particulières prescrites par celle-ci ;
– cessation par le bénéficiaire de l'exercice de l'activité pour laquelle l'autorisation lui a été délivrée.

S'y ajoute le retrait de plein droit en cas de condamnation du titulaire pour atteinte à la vie privée par captation de conversations privées ou atteinte au secret des correspondances.

Conformément à l'article R. 226-11 déjà cité, la procédure de retrait prévoit l'information préalable du titulaire, mis ainsi à même de faire valoir ses observations. Aucune règle spécifique n'a, par contre, été expressément prévue pour les refus. Ils sont donc motivés conformément aux règles de droit commun des actes administratifs et portés à la connaissance des demandeurs.

Depuis 1997, trois recours ont été formés devant un tribunal administratif contre des refus d'autorisation de détention d'un scanner. Ces requêtes ont été rejetées. Par ailleurs, la Commission européenne a été saisie de ce problème spécifique des scanners et de la non-conformité aux règles communautaires qui entacherait les restrictions imposées à leur égard par la France.

Ce type de matériel, récepteurs à large bande de fréquences, permet d'écouter des communications analogiques ainsi que les transmissions d'un certain nombre de services de secours ou de sécurité sur des fréquences réservées. Leur usage peut donc poser un problème de liberté individuelle et de

sécurité publique. Même s'il est possible de se les procurer par des voies parallèles, des conditions de délivrance strictes permettent de limiter les risques et contribuent à caractériser les intentions de tout détenteur irrégulier.

Enfin, les craintes de la CNCIS déjà exprimées dans les précédents rapports quant aux risques de violation de la vie privée subsistent. Sans doute les équipements peuvent-ils être achetés à distance ou sur des marchés occultes. Et les poursuites pénales sont rares, notamment contre les magasins vendant sans autorisation du matériel d'écoute, d'interception ou d'enregistrement ou contre leurs clients. Il faut toutefois signaler que la découverte sur l'internet d'une publicité proposant la vente de micro-émetteurs espions artisanaux a permis la saisie de plusieurs dizaines d'entre eux, d'un récepteur large bande permettant de les régler ainsi que d'un fichier de quelques dizaines de clients. La CNCIS ne peut que souhaiter la multiplication de procédures pénales de ce type et espérer qu'elles soient conduites jusqu'à leur terme.

Chapitre VIII

Les opérateurs

En matière d'interceptions de sécurité, le recours aux opérateurs est indispensable. Ce sont eux qui doivent assurer le renvoi de la ligne surveillée vers le site désigné par le service habilité [1].

Il n'a existé pendant de nombreuses années qu'un seul service de télécommunication, administration publique dépourvue de personnalité morale placée sous l'autorité du ministre chargé des postes et télécommunications. Ainsi, les interceptions étaient organisées et exécutées uniquement par des fonctionnaires appartenant à des services de l'État.

À partir des années 80 s'est engagé tant à l'échelon européen que national le processus qui allait bouleverser entièrement ce dispositif. Depuis le 1er janvier 1998, les télécommunications sont ouvertes à la concurrence et les acteurs de ce marché se comptent désormais par dizaines. Par ailleurs, des évolutions techniques, économiques et juridiques se sont produites à un rythme accéléré. Il convient donc de faire un point sur ces partenaires de l'État que sont les opérateurs.

Une grande diversité

L'opérateur est défini par l'article L. 32 du code des postes et télécommunications comme « une personne physique ou morale exploitant un réseau de télécommunications ouvert au public ou fournissant au public un service de télécommunications ». Ce même texte précise :

1) *Cf.* « le Groupement interministériel de contrôle » *in* CNCIS, 8ème rapport d'activité 1999, pages 41 et suivantes.

– « on entend par réseau de télécommunications toute installation ou tout ensemble d'installations assurant soit la transmission, soit la transmission et l'acheminement de signaux de télécommunications ainsi que l'échange des informations de commande et de gestion qui y est associé, entre les points de terminaison de ce réseau » ;
– « on entend par réseau ouvert au public tout réseau de télécommunications établi ou utilisé pour la fourniture au public de services de télécommunications » ;
– « on entend par services de télécommunications toutes prestations incluant la transmission ou l'acheminement de signaux ou une combinaison de ces fonctions par des procédés de télécommunication. Ne sont pas visés les services de communication audiovisuelle en tant qu'ils sont régis par la loi nº 86-1067 du 30 septembre 1986 ».

Alors que les procédés techniques peuvent être les mêmes, la distinction entre télécommunication et communication audiovisuelle réside dans la notion de correspondance privée ainsi que l'indique l'article 2 de la loi de 1986 relative à la liberté de communication. La correspondance est privée lorsque son destinataire est déterminé et individualisé, à la différence d'un message impersonnel adressé à l'ensemble des usagers ou clients d'un service audiovisuel.

Les jurisprudences du Conseil d'État et de la Cour de cassation précisent cette distinction. Par deux arrêts du 29 mai 1991 (Fédération nationale des radio-répondeurs et autres), le Conseil a indiqué « qu'il résulte de l'article 2 de la loi du 30 septembre 1986 relative à la liberté de communication que les services destinés à transmettre des correspondances privées entre les utilisateurs, au nombre desquels figurent les services de téléconvivialité permettant l'échange d'informations ou de messages entre utilisateurs sur le réseau téléphonique, ne constituent pas des services de communication audiovisuelle au sens de ladite loi ». La Cour, quant à elle, a précisé dans un arrêt du 25 octobre 2000 concernant une affaire pénale (*cf.* seconde partie de ce rapport) qu'un service de téléconvivialité télématique dont l'objet est de diffuser, à des personnes indifférenciées, des messages dont le contenu ne peut, par définition, être personnel, est bien un service de communication audiovisuelle « tant que l'auteur [d'une] annonce et l'un de ses lecteurs n'ont pas décidé de consentir à un dialogue ».

Pour exercer leurs activités, les opérateurs de réseaux doivent être autorisés par le ministre chargé des télécommunications en vertu de l'article L. 33-1 du code des postes et télécommunications ; les opérateurs de services doivent l'être également pour le service téléphonique au public (art. L. 34-1 du même code) mais sont libres [1] s'ils fournissent exclusivement des prestations autres que celui-ci (art. L. 34-2 du même code).

1) Exception faite des services utilisant des fréquences hertziennes ou des réseaux câblés.

Ces considérations juridiques, conjuguées aux progrès de la technologie, font que la variété des opérateurs est importante. En fin d'année 2000, on comptait 20 opérateurs de téléphones fixes titulaires de la licence « L. 33-1 », 21 de la licence « L. 34-1 » et 45 titulaires des deux, 11 opérateurs titulaires d'une licence de boucle locale et 12 opérateurs de mobiles et/ou de radiomessagerie [1].

S'agissant du téléphone fixe, France Télécom, opérateur historique, voit son ancien monopole d'accès aux abonnés attaqué de toutes parts, tout d'abord sur « la paire de cuivre » (qui assure le raccordement du téléphone filaire). Le décret 2000-881 du 12 septembre 2000 organise le dégroupage de l'accès à la boucle locale. Deux situations sont prévues : l'accès totalement dégroupé et l'accès partagé. Dans le premier cas, le nouvel opérateur peut utiliser l'intégralité de la bande de fréquences de la ligne et peut ainsi offrir un ensemble de services tant vocaux que de données. Dans le second cas, l'opérateur entrant dispose des fréquences non vocales de la ligne et peut, par exemple, mettre en œuvre des technologies telles l'ADSL pour proposer un accès à l'internet à haut débit. L'entrée en vigueur de ce texte a été fixée au 1er janvier 2001.

Différente du dégroupage mais toujours sur la paire de cuivre, l'offre en gros d'accès à haut débit permettra (quand les conditions, notamment tarifaires, seront déterminées aux nouveaux opérateurs) de proposer des services xDSL [2] en utilisant le réseau et les équipements de France Télécom.

Par ailleurs, des alternatives au raccordement filaire de l'utilisateur final se mettent en place. La plus connue d'entre elles est la boucle locale radio. Cette technique consiste à relier le client au réseau de l'opérateur par un faisceau hertzien. La relative simplicité de sa mise en place en fait, à terme, un concurrent sérieux du dégroupage filaire et particulièrement de l'offre xDSL dans la mesure où cette dernière technologie impose d'importantes contraintes de distance entre le client et le central téléphonique. Mais il est tout de même nécessaire que, dans le cas de la boucle locale radio, aucun obstacle important ne se trouve entre les deux extrêmités du faisceau. Les premières licences ont été attribuées dans le courant de l'été.

Deux autres possibilités sont la fibre optique et le service de la téléphonie vocale sur un réseau câblé de télédistribution. Pour offrir au public le service de la téléphonie, le câblo-opérateur doit être titulaire d'une autorisation « L. 34-1 » du code des postes et télécommunications (art. L. 34-4, al. 3 CP et T) tandis que pour les autres services de télécommunications, dont l'accès à l'internet, une simple déclaration suffit (même article, alinéa 1).

À côté du téléphone fixe et peut-être bientôt devant, le radiotéléphone a connu en 2000, et particulièrement au dernier trimestre, une accélé-

1) Source : Autorité de régulation des télécommunications (www.art-telecom.fr).
2) Sigle générique des technologies de transmission de données à haut débit sur la boucle locale, dont l'A.D.S.L. ou le S.D.S.L.

ration de sa croissance. Il équipe 29,68 millions de clients soit 49,4 % de la population française[5].

S'agissant des réseaux, la téléphonie mobile en 2000 s'est caractérisée par les premiers pas de l'UMTS. Rappelons que le lancement du projet d'un téléphone mobile de 3ème génération a été décidé par le Conseil et le Parlement européens en décembre 1998. Le terme imparti aux États est le 1er janvier 2002. En France, le Gouvernement a écarté la procédure de mise aux enchères et fait le choix de la sélection par soumission comparative en fixant le prix de la licence à 32,5 milliards de francs.

La promesse principale de cette nouvelle génération de radiotéléphone est le débit de transmission qui réalisera ce qu'il est convenu d'appeler l'internet mobile.

Si dans le langage courant le terme d'opérateur désigne généralement les seuls exploitants de réseaux, l'article L. 32 du code P et T nous indique que sont aussi des opérateurs les personnes physiques ou morales fournissant au public un service de télécommunications. On parle alors communément de « fournisseurs de services ».

Les plus facilement identifiables sont les titulaires d'une licence « L. 34-1 » c'est-à-dire ceux qui fournissant au public un service téléphonique.

Difficiles à répertorier exhaustivement sont les fournisseurs au public de services de télécommunications autres que le service téléphonique.

On peut classer dans cette catégorie les serveurs télématiques. On peut y ranger également ceux que l'on appelle les « intermédiaires techniques » de l'internet, à savoir les fournisseurs d'accès et les fournisseurs d'hébergement. Les fournisseurs de contenus ne satisfont pas quant à eux à la définition du service de télécommunications donnée plus haut, lequel doit inclure la transmission ou l'acheminement ou une combinaison de ces fonctions de signaux par des procédés de télécommunication. Ces différents types de fournisseurs sont parfois regroupés sous l'appellation de fournisseurs de services internet (FSI).

Une des principales questions les concernant est celle de leur responsabilité. L'actualité a donné des exemples de situations les mettant en cause : mise en consultation de photographies de célébrités à l'insu de celles-ci, accès à des sites de vente d'objets nazis...

La loi du 1er août 2000, déjà citée, a mis à la charge des fournisseurs d'accès une obligation d'information et de proposition de « moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner ». Elle encadre la responsabilité pénale ou civile des fournisseurs d'hébergement à raison des contenus au seul cas où « ayant été saisi[s] par une autorité judiciaire, [ils] n'ont pas agi promptement pour empêcher l'accès à ce contenu [1] ». Enfin, elle impose des délais de conservation des données de connexion. Un décret en Conseil d'État, pris après avis de la

Commission nationale de l'informatique et des libertés, doit définir les données et délais en cause.

Les derniers nés de la famille des fournisseurs de services sont les opérateurs mobiles virtuels, internationalement appelés MVNO [1]. S'appuyant sur le réseau d'un opérateur mobile, ils font une offre de fourniture de services à valeur ajoutée tout en gérant les cartes SIM [2] de leur clientèle. Inexistant en France, le concept est de façon générale très peu développé en Europe. Il mérite toutefois réflexion et observation dans la mesure où il risque d'engendrer des pratiques commerciales agressives vis-à-vis des opérateurs mobiles. Alors que les opérateurs mobiles et les opérateurs virtuels pourraient retirer, grâce au partage des coûts, un mutuel avantage de cette technologie, un déséquilibre au profit des opérateurs virtuels peut menacer la rentabilité des réseaux hôtes et, par là, freiner leur développement.

Des obligations réciproques

S'agissant des interceptions de télécommunications, les relations entre l'État et les opérateurs sont organisées sous deux aspects : d'une part, le droit pour les services habilités de solliciter les opérateurs ; et, d'autre part, l'obligation pour ceux-ci de satisfaire à ces demandes.

Les pouvoirs des services de l'État résultent d'un seul texte, la loi nº 91-646 du 10 juillet 1991 dont l'article 22 dispose que « 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 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. » L'article 11 de la loi précise que « 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. »

1) Mobile virtual network operator.
2) Subsciber identity module : carte à puce placée dans le téléphone et contenant les éléments relatifs à l'abonnement.

Les obligations qui pèsent sur les opérateurs sont issues de plusieurs textes. Les manquements sont constitutifs d'infractions et peuvent provoquer la suspension ou le retrait de la licence.

Le code des postes et télécommunications, modifié par la loi nº 96-659 du 26 juillet 1996 de réglementation des télécommunications, prévoit dans ses articles L. 33-1 et L. 34-1 que « ... l'autorisation [d'exploiter un réseau ouvert au public ou de fournir un service téléphonique ouvert au public] est soumise à l'application des règles contenues dans un cahier des charges et portant sur :

(...)

f) les prescriptions exigées par la défense et la sécurité publiques ;... »

Ce cahier des charges, outre des spécifications particulières, comporte des clauses types établies par l'article D. 98-1 du code des P et T au nombre desquelles les prescriptions suivantes : « l'opérateur se conforme aux décisions ou instructions des autorités judiciaires, militaires ou de police, ainsi qu'à celles du ministre chargé des télécommunications.

L'opérateur devra mettre en place et assurer la mise en œuvre des moyens nécessaires à l'application de la loi nº 91-646 du 10 juillet 1991 par les autorités habilitées en vertu de ladite loi... »

S'agissant de l'opérateur historique, son cahier des charges, approuvé par le décret nº 90-1213 du 29 décembre 1990 stipule en termes généraux qu'il doit « pouvoir répondre pour sa part aux besoins en matière de défense nationale et de sécurité publique... ».

Les opérateurs de fourniture au public de services de télécommunications autres que le service de la téléphonie sont soumis au « respect des exigences essentielles et des prescriptions relatives à la défense et à la sécurité publiques. » La reprise de la formulation utilisée pour les opérateurs soumis à autorisation indique sans ambiguïté que leurs obligations sont identiques.

Outre ces règles, s'imposent aux opérateurs quelques contraintes résultant de ce que les interceptions de sécurité sont couvertes par le secret de la défense nationale. C'est ainsi que les documents classifiés « secret-défense », tels les « cartons », doivent être transportés et conservés de façon spécifique, les locaux où sont traitées ces informations ainsi que les applications informatiques permettant d'assurer ce traitement, particulièrement sécurisés et les personnels appelés à en connaître, habilités.

La contrepartie accordée aux opérateurs est de deux ordres : premièrement, accomplissant des actes prescrits ou autorisés par des dispositions législatives ou réglementaires, ils ne sont pas, suivant l'article 122-4 du code pénal, pénalement responsables d'atteintes au secret des correspondances ou à la vie privée ; en second lieu, ils ont droit à une « juste rémunération des prestations assurées » (art. L. 35-6 CP et T).

Cette rémunération doit faire l'objet d'une convention entre l'État et les opérateurs. Sont visés les études, l'ingénierie, la conception, le déploiement et l'exploitation des systèmes demandés.

La deuxième loi de finances rectificative pour 2000 comportait, dans son article 48, des dispositions mettant à la charge des opérateurs les investissements nécessaires aux interceptions et ne prévoyait, en ce qui concerne les charges d'exploitation, qu'une participation de l'État. Ces dispositions ont été déclarées non conformes à la Constitution par une décision du Conseil constitutionnel en date du 28 décembre 2000, par le motif que « le concours ainsi apporté à la sauvegarde de l'ordre public, dans l'intérêt général de la population, est étranger à l'exploitation des réseaux de télécommunication ; que les dépenses en résultant ne sauraient dès lors, en raison de leur nature, incomber directement aux opérateurs ».

Perspectives d'avenir

En matière de défense et de sécurité publique, l'avenir des relations entre l'État et les opérateurs se joue actuellement au niveau international dans différentes enceintes : le G8, le Conseil de l'Europe et l'Union européenne.

La préoccupation dominante concerne les systèmes et réseaux de données informatiques, notamment du fait de l'absence de cadre juridique précis pour les intermédiaires de l'internet.

Les réflexions menées par le G8 [1] ont conduit en décembre 1997, à Washington, les ministres de la justice et de l'intérieur de ces pays à établir un programme d'action contre le « cybercrime ». Le point nº 7 est ainsi libellé : « œuvrer conjointement avec le secteur industriel pour veiller à ce que les nouvelles technologies facilitent la lutte contre le crime technologique en assurant la préservation et le recueil des éléments de preuve critiques ».

Alors que les travaux des instances internationales sont généralement internes, le G8 a souhaité y associer les industriels. C'est ainsi qu'a été organisée à Paris du 15 au 17 mai 2000 la première conférence réunissant des représentants des États et des entreprises, industriels ou intermédiaires tels les fournisseurs d'accès à l'internet.

Dans la lutte contre le cybercrime, l'intérêt des États est double. Ils doivent tout d'abord se protéger eux-mêmes contre les utilisations attentatoires des nouvelles technologies de l'information et de la communication ; ils assurent également la protection de l'ordre public ainsi que de leurs ressortissants ou des agents économiques opérant sur leur territoire contre les utilisations illégales ou préjudiciables de ces technologies.

1) Allemagne, Canada, Etats-Unis, France, Italie, Japon, Royaume-Uni et Russie.

Les représentants des États ont indiqué aux entreprises qu'outre la conception et le fonctionnement des infrastructures et des systèmes, elles devaient assumer la responsabilité première de la sécurité des réseaux. Ils attendent donc des entreprises qu'elles mettent en œuvre leur capacité de recherche et d'innovation afin de trouver des solutions techniques non seulement de protection, mais aussi de détection et d'alerte.

De leur côté, les entreprises et notamment les fournisseurs d'accès ou d'hébergement ont fait part de leur refus de se transformer en auxiliaires de police. Si dans certains pays des associations professionnelles ont établi des règles de conduite relatives au traitement des demandes émanant des autorités d'enquête, ces mêmes associations ont alerté les pouvoirs publics sur le risque qu'un cadre juridique trop contraignant ferait courir au développement de l'internet et particulièrement du commerce électronique.

Le Conseil de l'Europe quant à lui travaille à l'élaboration d'une convention sur la cybercriminalité. Le projet (version nº 25 [1]) prévoit, notamment, à son titre 5, la collecte en temps réel de données informatiques. Il s'agit de données relatives soit au trafic (article 20) soit au contenu (article 21). Dans les deux cas, chaque État doit prendre les mesures juridiques nécessaires pour permettre à ses services habilités « d'obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes à :
– collecter ou à enregistrer par application de moyens sur son territoire, ou
– prêter aux autorités compétentes coopération et assistance pour la collecte ou l'enregistrement, en temps réel, de données relatives [au trafic ou au contenu] et en rapport avec des communications précises sur son territoire transmises au moyen d'un système informatique. »

Au sein de l'Union européenne, enfin, trois documents témoignent de l'intérêt des États pour les interceptions de télécommunications : la Convention d'entraide judiciaire en matière pénale du 29 mai 2000, la proposition de directive concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques du 12 juillet 2000, la communication de la Commission européenne en date du 26 janvier 2001 en vue de créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité.

L'un des aspects du premier de ces textes, la Convention d'entraide, est d'organiser la coopération entre États membres de l'Union européenne en matière d'interceptions de télécommunications. Elle n'aura en fait pas ou peu d'incidences sur les rapports entre opérateurs et autorités publiques. Tel n'est pas le cas des deux autres.

La proposition de directive sur le traitement des données à caractère

1) http : //conventions.coe.int/treaty/FR/projets/cybercrime25.htm.

personnel est destinée à moderniser la directive 97/66/CE [1] en fonction de l'état actuel et prévisible des technologies des télécommunications. Elle comporte notamment l'indication suivante : « à l'instar de la directive 95/46/CE, la présente directive ne traite pas des questions de protection des droits et libertés fondamentaux liés à des activités qui ne sont pas régies par le droit communautaire. Il appartient aux États membres de prendre les mesures 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. La présente directive ne porte pas atteinte à la faculté des États membres de procéder aux interceptions légales des communications électroniques justifiées par rapport à l'un des buts précités. »

Enfin, dans sa communication du 26 janvier 2001, la Commission européenne note que si des relations ont déjà été nouées entre les opérateurs « traditionnels » de téléphonie vocale et les autorités publiques chargées des interceptions de télécommunications, des discussions doivent être menées avec l'ensemble des nouvelles entreprises du marché ainsi qu'avec les autorités de contrôle chargées de la protection des données (en France, la CNIL) sur les questions de la réglementation, de la faisabilité technique, de la répartition des coûts et de l'impact commercial. En raison de l'internationalisation des réseaux et particulièrement de l'internet, la Commission ajoute que les obligations technologiques susceptibles d'être imposées par les États aux entreprises de télécommunications ou aux fournisseurs de services devraient être harmonisées.

1) Directive 97/66/CE du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications. Cette directive a traduit à ce secteur les principes de la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Chapitre IX

Le point sur la jurisprudence de la Cour européenne des droits de l'Homme en matière d'écoutes téléphoniques

I – Le rapport annuel de la CNCIS a comporté régulièrement, depuis la création de la Commission jusqu'en 1998, une rubrique sur la jurisprudence de la Cour européenne des droits de l'Homme (CEDH). Il l'aurait fait aussi en 1999 si la Cour avait, cette année-là, rendu une décision en matière d'écoutes téléphoniques. On trouvera, dans le présent rapport, le texte des extraits de deux arrêts de la CEDH intervenus dans ce domaine en 2000.

La CNCIS se devait d'être attentive à cette jurisprudence non seulement pour son intérêt intrinsèque, mais aussi par un sentiment de fidélité. La loi du 10 juillet 1991, qui crée notamment cette commission, trouve en effet son origine dans deux décisions de la CEDH rendues le même jour (24 avril 1990), et, en droit, dans les mêmes termes : les décisions Huvig et Kruslin. Prises à propos d'interceptions judiciaires, elles étaient aussi applicables aux interceptions administratives, les unes et les autres tombant sous le coup de la même critique : le droit français – résume en effet la Cour – « n'indique pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir appréciation des autorités dans le domaine considéré ». Il est vrai qu'à l'époque, les interceptions judiciaires n'avaient d'autre fondement légal que l'article 81 du code de procédure pénale, aux termes duquel « le juge d'instruction procède, conformément à la loi, à tous les actes qu'il juge utiles à la manifestation de la vérité ». Quant aux interceptions administratives, elles

n'étaient organisées que par une circulaire, la « circulaire Debré » du 28 mars 1960, classée « très secret » et déclassée en 1992 afin d'être reproduite dans le premier rapport de la CNCIS.

En 1990, quand l'état du droit en France a été examiné et critiqué par la CEDH, sa pensée avait eu l'occasion de s'affirmer et de s'affiner depuis assez longtemps, puisque la première décision en la matière date de 1978. Des affaires nouvelles ont été jugées jusqu'à la fin du siècle, et le moment paraît venu de présenter cette jurisprudence dans son ensemble.

II – La Cour a examiné une quinzaine de recours relatifs à des interceptions. Cinq de ses arrêts tranchent des questions de principe et appellent un commentaire.

1 – *L'arrêt Klass c. République Fédérale d'Allemagne*, de 1978, pose en principe que l'article 8 de la Convention européenne des droits de l'Homme et des libertés fondamentales, lorsqu'il proclame dans son paragraphe 1 que « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance », englobe dans son champ d'application les conversations téléphoniques, même si elles n'y sont pas expressément mentionnées.

Quant au paragraphe 2 de l'article 8, il dispose que l'ingérence de l'autorité publique dans l'exercice de ce droit ne peut se justifier dans une société démocratique que lorsqu'elle est nécessaire, notamment à la sécurité nationale, à la défense de l'ordre et à la prévention des infractions pénales. Mais la Cour souligne que l'autorité ne dispose pas pour autant d'une latitude illimitée, et qu'elle ne saurait « détruire la démocratie au motif de la défendre ». La Cour se livre donc à un examen détaillé de la situation de droit et de fait afin de vérifier si la conciliation entre les impératifs de défense d'une société démocratique et de sauvegarde des droits individuels est assurée. Cette conciliation doit prendre en compte un danger d'arbitraire d'autant plus net que le pouvoir de l'exécutif, en matière d'écoutes, s'exerce en secret.

2 – *L'arrêt Malone c. Royaume Uni*, de 1984, interprète la disposition de l'article 8 § 2, de la convention selon laquelle les ingérences doivent être « prévues par la loi ». Tout en confirmant une jurisprudence, afférente à un autre article, selon laquelle la « loi » englobe à la fois le droit écrit et le droit non écrit, la Cour juge particulièrement utile d'exiger, dans le domaine des interceptions, comme dans d'autres cas où c'est la liberté d'expression qui est en cause, que la loi soit suffisamment précise. La loi applicable au Royaume Uni, datant de 1969, comportait des dispositions assez obscures et sujettes à des analyses divergentes : la condition prévue par l'article 8 § 2 n'était donc pas remplie.

3 – *Les décisions Huvig et Kruslin c. France* de 1990 se situent, on l'a dit, sur le même terrain, celui de la « qualité » de la loi. La Cour a admis que les interceptions judiciaires avaient une base légale en droit français. Mais elle a estimé que cette base n'était pas compatible avec la « prééminence du

droit », autrement dit qu'elle ne présentait pas les qualités requises, et ce pour deux raisons : d'une part la jurisprudence développée sur la base du texte très bref du code de procédure pénale n'avait pas explicitement consacré les garanties nécessaires, ou encore était intervenue dans des domaines autres que celui des écoutes ; d'autre part et surtout, le système établi par la loi et la jurisprudence ne comportait pas diverses précisions indispensables, notamment quant aux catégories de personnes susceptibles d'être mises sur écoute, à la nature des infractions permettant d'y recourir, à la durée de la mesure, à la sauvegarde des enregistrements, à leur effacement ultérieur.

4 – *L'arrêt Halford c. Royaume Uni* de 1997 statue d'abord sur l'existence d'une « ingérence », au sens de l'article 8 de la Convention, dans un cas où l'écoute a porté sur une conversation passée sur un téléphone de bureau. La réponse est affirmative, notamment parce que l'utilisatrice n'avait pas été prévenue que ses appels étaient susceptibles d'être interceptés, et que les interceptions tendaient à fournir à son employeur des informations pour étayer sa défense dans une procédure intentée contre lui par Madame Halford.

D'autre part, le téléphone de bureau en cause était connecté sur un réseau de télécommunications indépendant du réseau public, le seul auquel s'appliquait la loi de 1985 sur les interceptions. L'ingérence n'était donc pas « prévue par la loi » au sens de l'article 8 § 2, dès lors que le droit interne n'offrait aucune protection à Madame Halford. Il ne lui offrait, notamment, aucune possibilité de recours devant une instance nationale, et méconnaissait donc aussi l'article 13 de la Convention.

5 – *L'arrêt Kopp c. Suisse* de 1998 est intervenu à propos de l'interception des communications téléphoniques d'un avocat. La loi suisse protège la confidentialité des relations entre un avocat et ses clients. Mais toutes les lignes téléphoniques du cabinet avaient été surveillées, et donc toutes les conversations, quelles qu'elles soient, écoutées. Se posait alors un problème de qualité de la loi : si le secret professionnel couvre bien l'activité en cause, la loi ne dit ni comment ni par qui doit s'opérer le tri entre ce qui relève de cette activité et ce qui lui est étranger, lacune d'autant plus fâcheuse qu'elle touche aux droits de la défense. En tant qu'avocat, M. Kopp n'a donc pas joui de la protection exigée par la « prééminence du droit » dans une société démocratique.

III – De la jurisprudence ainsi résumée, il se dégage que l'interception téléphonique constitue toujours une ingérence de l'autorité publique dans le droit au respect de la vie privée et de la correspondance. Une telle ingérence méconnaît l'article 8 § 2 sauf si des conditions de forme et de fond sont réunies.

Il faut d'abord que la mesure soit « prévue par la loi », formule qui recouvre plusieurs exigences :
– d'abord, l'existence d'une loi, et aussi son accessibilité, condition qui apparemment, n'a jamais fait défaut dans les affaires jugées par la Cour ;

– il faut en outre, que la loi soit « prévisible », selon le terme employé par la Cour, c'est-à-dire que les personnes concernées puissent en prévoir les conséquences pour elles, ce qui suppose que ses dispositions soient claires et détaillées et qu'elles comportent les garanties permettant d'éviter les abus.

Quant aux exigences de fond, elles sont précisées dans l'article 8 § 2 : il faut que des menaces pèsent sur les intérêts fondamentaux que constituent la sécurité nationale, la sûreté publique, le bien-être économique de pays, la défense de l'ordre, la prévention des infractions pénales, la protection de la santé ou de la morale, la protection des droits et libertés d'autrui : liste si longue, aux termes si larges, qu'il y a peu de chance que ses limites soient méconnues ; mais il faut, de plus, que l'interception soit « nécessaire dans une société démocratique », ce qui ouvre à l'évidence un champ plus vaste au contrôle de la CEDH.

Chapitre X

Le régime juridique des interceptions de sécurité à la lumière de l'expérience allemande

La CNCIS s'est rendue à Hambourg en mai 2000 pour rencontrer son homologue allemande, la Commission G10 du Bundestag. Cette visite était également l'occasion de rendre hommage à son ancien Président, M. Arndt, qui avait dirigé cette instance pendant 30 ans.

Le système allemand de contrôle des interceptions administratives comprend à la fois une commission fédérale et des commissions propres à chaque Land. Ce déplacement a donc également permis un échange avec les membres de la commission de Hambourg et une visite au service des renseignements intérieurs de ce Land (Landesamt für Verfassungsschutz). La commission fédérale G10 est compétente pour les interceptions demandées par les trois services de renseignements fédéraux chargés respectivement du renseignement intérieur, du renseignement militaire et du renseignement extérieur. Les commissions des Länder font le même travail pour celles demandées par le service de renseignement intérieur de chacun d'eux. Une concertation permanente s'établit entre la commission du Bundestag et celles des Länder, notamment pour le traitement des réclamations de particuliers.

L'objet du présent chapitre est de mettre en exergue les particularités du système allemand par rapport à la législation française, alors même que dans les faits, les pratiques relevées et l'exercice du contrôle révèlent de nombreux points communs dans le traitement des interceptions administratives des deux Etats.

Une législation détaillée et évolutive

La loi allemande, dite loi G10, est entrée en vigueur le 1er novembre 1968, elle a donc plus de trente ans d'existence, ce qui en fait l'une des législations les plus anciennes en la matière.

Elle a été complétée et précisée à plusieurs reprises, et notamment en 1978, d'une part par l'obligation d'informer, après l'expiration de la mesure, la personne qui en a été l'objet, à condition toutefois de ne pas risquer de compromettre l'objectif poursuivi, et d'autre part par l'affirmation de principe qu'une atteinte au secret des correspondances ne pouvait avoir lieu sans une autorisation préalable de la commission G10. Le corollaire de cette exigence a été la création d'une procédure dérogatoire pour l'urgence.

La loi allemande a ensuite successivement pris en compte les évolutions économiques, techniques, juridiques : en 1989, l'obligation faite à la Deutsche Bundespost de participer aux mesures d'interception a été élargie aux autres opérateurs, y compris les opérateurs privés, à la suite de l'ouverture à la concurrence du secteur des télécommunications ; en 1990, la loi a été modifiée pour permettre la surveillance des télécommunications faisant appel à de nouvelles technologies ; en 1992, la question des compétences respectives de la commission G10 et du Commissaire à la protection des données nominatives, en matière de surveillance des télécommunications, a été réglée en faveur de la première par une disposition législative faisant application du principe de spécialité.

Enfin, la prise en compte des nouvelles formes de l'insécurité en Europe a conduit depuis une dizaine d'années à l'élargissement des motifs justifiant le recours au « contrôle stratégique », c'est-à-dire à la surveillance exercée sur certaines liaisons entre l'Allemagne et l'étranger, destinée à collecter des informations non individualisées pour prévenir certaines menaces.

Un contrôle spécifique au sein du contrôle parlementaire des services de renseignement

À la différence de la CNCIS qui est une autorité administrative indépendante, la commission fédérale G10 est une émanation du Bundestag. Son budget est pris sur celui de cette assemblée. Ses membres (4 titulaires et 4 suppléants) sont désignés par l'organe de contrôle parlementaire des services de renseignement (PKG) après avis du Gouvernement, qui procède à une enquête de sécurité.

Le PKG, élu lui-même au sein du Bundestag, est en charge du contrôle général de l'activité des trois services de renseignement fédéraux. Il donne son avis sur leurs budgets et est informé de leur exécution. Dans le cadre de ce contrôle, il reçoit tous les semestres un compte rendu du ministre fédéral

de l'intérieur sur les interceptions de correspondance intervenues, leur exécution, les résultats qu'elles ont permis d'obtenir. Ce compte rendu ne porte pas sur les mesures individuelles mais évoque les questions de principe posées par l'application de la loi relative aux atteintes légales au secret des correspondances prise en application de l'article 10 de la Constitution. Le PKG soumet au Bundestag en milieu et en fin de législature un rapport sur son activité de contrôle et doit lui présenter annuellement un rapport spécifique sur l'exécution des écoutes stratégiques.

La commission G10 décide si les mesures d'interception soumises par le ministre fédéral compétent sont nécessaires et conformes aux exigences légales. Elle contrôle également la régularité de l'exécution et s'assure que les destructions des enregistrements, transcriptions, supports informatiques prévues par la loi sont effectives et que les dispositions relatives à l'information a posteriori des personnes ayant fait l'objet d'une surveillance de leur correspondance sont respectées. Elle peut entreprendre des vérifications soit d'initiative, soit sur la base de plaintes de particuliers qu'elle instruit. Son champ d'intervention recoupe donc étroitement celui de la CNCIS.

La composition de la commission G10 reflète celle du Bundestag : ses membres sont désignés par les partis de la majorité ou de l'opposition. Le président et son suppléant doivent être aptes aux fonctions de magistrat. Irrévocables, les membres de la commission ne peuvent recevoir d'instruction de quiconque. Ces caractéristiques les rapprochent des membres de la commission française. Toutefois leur mandat se perpétue au-delà d'une législature pour une durée maximale de trois mois afin de permettre l'élection de leurs successeurs. Ils peuvent être renouvelés dans leur fonction, ce qu'interdit le système français, et ils le sont assez fréquemment. Les membres de la commission allemande peuvent être parlementaires ; en revanche, comme les membres de la CNCIS, ils ne peuvent en même temps appartenir au Gouvernement.

Les deux commissions répondent ainsi aux mêmes types de préoccupations : volonté d'associer le Parlement dans toutes ses composantes, volonté d'assurer l'indépendance de l'instance de contrôle par un statut d'irrévocabilité.

Certes les deux commissions s'inscrivent l'une dans un contexte de contrôle parlementaire des services de renseignement, l'autre hors de ce contexte, mais elles exercent dans les faits un rôle sensiblement équivalent sur une activité bien circonscrite par la loi.

Une commission de contrôle indépendante, détentrice du pouvoir d'autorisation

À la différence de la commission française dont le rôle est consultatif aux termes de la loi, le rôle décisionnel de la commission allemande est expressément inscrit dans les textes depuis que la réforme de 1978 en a entériné la pratique. Aucune mesure de surveillance des correspondances ne peut être faite sans son autorisation préalable. Dans l'hypothèse d'urgence, l'interception est mise en œuvre à la demande du ministre fédéral de la défense ou de l'intérieur mais doit être soumise sans délai à la commission G10. En cas de décision négative de cette dernière, l'exécution de la mesure doit être immédiatement interrompue. Les décisions de la commission ne sont pas susceptibles de recours. Rappelons qu'en France, depuis plusieurs années l'avis négatif de la CNCIS est toujours suivi, mais une pratique différente pourrait être rétablie.

Les décisions de la commission G10 sont collégiales : elle ne peut délibérer valablement que si quatre de ses membres titulaires ou suppléants sont présents. Elle travaille dans le secret et sous sa propre responsabilité, ne peut recevoir d'instruction de quiconque et ne rend compte à personne de son activité. Elle ne peut communiquer d'élément sur le nombre d'interceptions, à la différence de la CNCIS qui aux termes de la loi rend compte annuellement de son activité dans son rapport public et consacre toujours une partie de son compte rendu aux statistiques. Les rapports présentés par l'organe de contrôle parlementaire PKG assurent cependant une transparence certaine au système de surveillance allemand, transparence à laquelle contribue, à un autre niveau, l'obligation de porter à la connaissance des particuliers qui en ont été l'objet la mesure d'interception.

Une procédure d'autorisation et un contrôle de l'exécution très comparables

Si l'on fait abstraction du fait que les interceptions, en Allemagne, peuvent porter sur les correspondances postales, la procédure d'autorisation est proche de celle de la loi française du 10 juillet 1991 : demandes motivées et écrites présentées par les services, transmission par les ministres compétents, chaque mois, à la commission G10 pour autorisation, exécution par le canal des opérateurs de télécommunications. Les motifs légaux de recours aux mesures d'interception des correspondances, bien que présentés différemment dans la loi allemande, recouvrent largement ceux qu'énumère la loi française. La législation allemande s'attache aussi à définir les personnes susceptibles d'être les cibles de ces mesures, ce que ne fait pas la loi française qui n'évoque que les motifs justifiant l'interception. Cette différence doit être relativisée dans la pratique, car pour apprécier le bien fondé d'un motif, il est indispensable de prendre en considération la personne visée autant que les éléments qui constituent le fondement légal du

recours à l'interception. En revanche, à la différence du système allemand, la loi française prévoit le contingentement des interceptions.

En l'absence d'un organisme chargé de centraliser l'exécution des interceptions comme le GIC en France, la commission G10 est amenée à exercer son contrôle directement dans les installations des services utilisateurs et chez les opérateurs de télécommunications. Ses pouvoirs d'investigation, le contrôle qu'elle exerce sur l'exécution, le traitement des plaintes de particuliers sont comparables à ceux de la CNCIS. L'absence d'un GIC dans le système allemand est compensée par le fait que les services autorisés à recourir à des interceptions sont seulement au nombre de trois.

Le « contrôle stratégique »

Si la loi française n'évoque que « les interceptions de correspondance émises par voie des télécommunications » (titre II de la loi) et « les mesures de surveillance prises aux seules fins de défense des intérêts nationaux des transmissions empruntant la voie hertzienne », ces dernières échappant au régime des interceptions de sécurité et au contrôle de la CNCIS, la loi allemande a un domaine plus large.

Elle distingue en effet deux types de surveillance légale des correspondances suivant l'objectif poursuivi. Il s'agit d'une part, des mesures visant les correspondances d'une personne pour laquelle il existe des indices de commission d'infractions dont la liste est fixée par l'article 1, paragraphe 2 (1) de la loi du 13 août 1968, (ce type de surveillance englobant aussi les correspondances postales) d'autre part, des surveillances dites stratégiques, destinées non pas à surveiller des personnes mais à collecter sur certaines liaisons internationales des informations matérielles et objectives permettant en temps utile d'identifier les menaces extérieures susceptibles de créer un danger pour l'Allemagne. La nature de ces menaces pour la sécurité allemande est prévue par le paragraphe 3 (1) du même article : agression armée, attentats terroristes sur le territoire allemand, trafic international de matériel de guerre ou de moyens de destruction massive bactériologique, chimique ou nucléaire ou encore de stupéfiants, blanchiment d'argent, faux monnayage. La surveillance ne doit pas permettre de retenir des éléments contre des personnes identifiées.

Le contrôle stratégique suppose que l'arrivée ou le point de départ de la liaison observée se situe à l'étranger, dans des zones à risque pour la sécurité allemande définies par un arrêté du ministre fédéral de la Défense approuvé par le PKG. La commission G10 exerce sa compétence sur les mesures de contrôle stratégique.

L'obligation de notification

S'agissant des mesures individuelles, le ministre fédéral allemand compétent doit informer la personne qui en a été l'objet que cette mesure a pris fin. Tous les mois sont ainsi présentées à la commission du G10, outre les projets d'interception, les notifications effectuées et les cas dans lesquels cette obligation de notification se heurte à des objections susceptibles d'y faire obstacle. En effet, si la notification est de nature à remettre en cause l'objectif poursuivi par la mesure, la commission peut exceptionnellement dispenser le gouvernement de notifier ou décider qu'il sera sursis à cette démarche. Il n'y a pas de notification dans le cas du contrôle stratégique puisqu'il ne comporte pas de contrôle individualisé. S'il advient qu'à l'occasion de la surveillance des transmissions hertziennes internationales, certaines personnes sur le territoire allemand soient interceptées, les informations collectées doivent être détruites dans un délai de trois mois, faute de quoi notification devra être faite aux intéressés de l'atteinte qu'ils ont subie au secret de leurs communications. La notification peut être exclue ou retardée dans les mêmes conditions que celles prévues pour les mesures individuelles.

Cette règle de notification alimente des recours contentieux devant les juridictions administratives qui, dans la quasi totalité des cas, ont été rejetés.

La loi française ne prévoit pas ce type de disposition mais permet à la CNCIS, agissant soit d'initiative, soit à la suite d'une enquête consécutive à une réclamation, de dénoncer au procureur de la République les infractions à la loi du 10 juillet 1991 qu'elle aurait constatées. La commission G10 dispose pour sa part de la possibilité de saisir le ministre fédéral de la justice (ou celui du Land pour les commissions régionales) lorsqu'elle découvre des écoutes illégales.

* * *

Rattachement de la Commission en charge des écoutes au Parlement ; compétence de cette commission en matière de « contrôle stratégique » ; notification a posteriori de l'interception à la personne écoutée : tels sont les traits essentiels qui distinguent le système allemand du système français. Mais la CNCIS a eu le sentiment que la différence principale était de nature psychologique, et qu'elle tenait à une attitude beaucoup plus simple et ouverte des Allemands sur ces questions. C'est probablement parce que sa législation est plus ancienne que la nôtre : elle a eu plus de temps pour obtenir, dans l'esprit public, des effets positifs que la loi française de 1991 commence seulement à produire.

Deuxième partie

ÉTUDES ET DOCUMENTS

Textes

Plusieurs textes dont une proposition de loi ont retenu plus particulièrement l'attention de la CNCIS cette année par la proximité de leur objet avec sa propre activité.

Il s'agit tout d'abord des dispositions de la Convention relative à l'entraide judiciaire en matière pénale en ce qu'elle consacre un titre III aux interceptions des télécommunications, de la Convention des Nations Unies contre la criminalité transnationale organisée qui consacre un article 20 aux techniques d'enquêtes spéciales et de la loi 2000-494 portant création d'une Commission nationale de déontologie de la sécurité.

Il convient également de souligner l'existence d'une proposition de loi tendant à la création de délégations parlementaires pour le renseignement adopté par la commission de la défense nationale de l'Assemblée nationale sur proposition de M. Paul Quilès et plusieurs de ses collègues.

Conseil européen, convention du 29 mai 2000 relative à l'entraide judiciaire en matière pénale

Titre III
Interception des télécommunications

Article 17
Autorité compétente pour ordonner l'interception de télécommunications

Aux fins de l'application des dispositions des articles 18, 19 et 20, on entend par « autorité compétente » une autorité judiciaire ou, lorsque les autorités judiciaires ne sont pas compétentes dans le domaine couvert par lesdites dis-

positions, une autorité compétente équivalente désignée conformément à l'article 24, paragraphe 1, point e), et agissant aux fins d'une enquête pénale.

Article 18
Demandes d'interception de télécommunications

1 – Une autorité compétente de l'État membre requérant peut, pour les besoins d'une enquête pénale et conformément aux exigences de sa législation nationale, adresser à une autorité compétente de l'État membre requis une demande en vue :
a) – de l'interception de télécommunications et de leur transmission immédiate à l'État membre requérant, ou
b) – de l'interception, de l'enregistrement et de la transmission ultérieure de l'enregistrement de télécommunications à l'État membre requérant.

2 – Des demandes au titre du paragraphe 1 peuvent être présentées, en ce qui concerne l'utilisation de moyens de télécommunication par la cible de l'interception, si celle-ci se trouve dans :
a) – l'État membre requérant, et lorsque celui-ci a besoin de l'aide technique de l'État membre requis pour pouvoir intercepter les communications de la cible ;
b) – l'État membre requis, et lorsque les communications de la cible peuvent être interceptées dans cet État ;
c) – dans un État membre tiers, qui a été informé conformément à l'article 20, paragraphe 2, point a), et lorsque l'État membre requérant a besoin de l'aide technique de l'État membre requis pour intercepter les communications de la cible.

3 – Par dérogation à l'article 14 de la Convention européenne d'entraide judiciaire et à l'article 37 du traité Benelux, les demandes présentées en application du présent article doivent :
a) – indiquer l'autorité qui présente la demande ;
b) – confirmer qu'un ordre ou un mandat d'interception régulier a été émis dans le cadre d'une enquête pénale ;
c) – contenir des informations permettant d'identifier la cible de l'interception ;
d) – indiquer le comportement délictueux faisant l'objet de l'enquête ;
e) – mentionner la durée souhaitée de l'interception ; et
f) – si possible, contenir des données techniques suffisantes, en particulier le numéro pertinent de connexion au réseau, pour permettre le traitement de la demande.

4 – Lorsque la demande est présentée en vertu du paragraphe 2, point b), elle doit aussi contenir une description des faits. L'État membre requis peut demander toute information supplémentaire qui lui paraît nécessaire pour lui permettre d'apprécier si la mesure requise serait prise dans une affaire nationale similaire.

5 – L'État membre requis s'engage à faire droit aux demandes présentées au titre du paragraphe 1, point a) :
a) – lorsque la demande est présentée en vertu du paragraphe 2, points a) et c), dès qu'il a reçu les informations énumérées au paragraphe 3. L'État membre requis peut autoriser l'interception sans plus de formalités ;

b) – lorsque la demande est présentée en vertu du paragraphe 2, point b) dès qu'il a reçu les informations visées aux paragraphes 3 et 4 et lorsque la mesure requise serait prise dans une affaire similaire. L'État membre requis peut subordonner son accord au respect des conditions qui devraient respectées dans une affaire nationale similaire.

6 – Lorsque la transmission immédiate n'est pas possible, l'État membre requis s'engage à donner suite aux demandes adressées au titre du paragraphe 1, point b), dès qu'il a reçu les informations visées aux paragraphes 3 et 4 et lorsque la mesure requise serait prise dans une affaire nationale similaire. L'État membre requis peut subordonner son accord au respect des conditions qui devraient respectées dans une affaire nationale similaire.

7 – Au moment de la notification visée à l'article 27 du paragraphe 2, un État membre peut déclarer qu'il n'est lié par le paragraphe 6 que lorsqu'il n'est pas en mesure d'assurer une transmission immédiate. En pareil cas, les autres États membres peuvent appliquer le principe de réciprocité.

8 – Lorsqu'il formule une demande au titre du paragraphe 1, point b) l'État membre requérant peut, s'il a une raison particulière de le faire, demander également une transmission de l'enregistrement. L'État membre requis examine ces demandes conformément à sa législation et à ses procédures nationales.

9 – L'État membre qui reçoit les informations communiquées en vertu des paragraphes 3 et 4 les traite de manière confidentielle conformément à sa législation nationale.

Article 19
Interception de télécommunications sur le territoire national par l'intermédiaire des fournisseurs de services

1 – Les États membres veillent à ce que les systèmes de services de télécommunications qui opèrent sur leur territoire via une station terrestre et qui, aux fins de l'interception légale des communications d'une cible présente dans un autre État membre, ne sont pas directement accessibles pour les besoins de l'interception légale par ledit État membre par l'intermédiaire d'un fournisseur de services désigné présent sur son territoire.

2 – Dans le cas visé au paragraphe 1, les autorités compétentes d'un État membre peuvent, pour les besoins d'une enquête pénale, conformément à la législation nationale applicable et à condition que la cible de l'interception soit présente dans cet État membre, procéder à l'interception par l'intermédiaire d'un fournisseur de services désigné présent sur son territoire sans faire intervenir l'État membre sur le territoire duquel se trouve la station terrestre.

3 – Le paragraphe 2 s'applique également lorsqu'il est procédé à l'interception à la suite d'une demande présentée au titre de l'article 18, paragraphe 2, point b).

4 – Rien dans le présent article n'empêche un État membre de présenter à l'État membre sur le territoire duquel se trouve la station terrestre une demande d'interception légale de télécommunications conformément à l'ar-

ticle 18, en particulier lorsqu'il n'existe pas d'intermédiaire dans l'État membre requérant.

Article 20
Interception de télécommunications sans l'assistance technique d'un autre État membre

1 Sans préjudice des principes généraux du droit international ainsi que des dispositions de l'article 18, paragraphe 2, point c), les obligations prévues dans le présent article s'appliquent aux ordres d'interception donnés ou autorisés par l'autorité compétente d'un État membre dans le cadre d'enquêtes pénales présentant les caractéristiques d'une enquête menée lorsqu'a été commise une infraction pénale déterminée, y compris les tentatives dans la mesure où elles sont incriminées dans le droit national, aux fins d'identification et d'arrestation, d'accusation, de poursuite ou de jugement des responsables.

2 – Lorsque l'autorité compétente d'un État membre qui effectue l'interception (« l'État membre interceptant ») a autorisé, pour les besoins d'une enquête pénale, l'interception de télécommunications et que l'adresse de télécommunication de la cible visée dans l'ordre d'interception est utilisée sur le territoire d'un autre État membre (« l'État membre notifié ») dont l'assistance technique n'est pas nécessaire pour effectuer cette interception, l'État membre interceptant informe l'État membre notifié de l'interception :

a) avant l'interception dans les cas où il sait déjà au moment d'ordonner l'interception que la cible se trouve sur le territoire de l'État membre notifié ;

b) dans les autres cas, dès qu'il s'aperçoit que la cible de l'interception se trouve sur le territoire de l'État membre notifié.

3 – Les informations notifiées par l'État membre interceptant doivent notamment :

a) indiquer l'autorité qui ordonne l'interception ;

b) confirmer qu'un ordre d'interception régulier a été émis dans le cadre d'une enquête pénale ;

c) contenir des informations permettant d'identifier la cible de l'interception ;

d) indiquer l'infraction faisant l'objet de l'enquête ;

e) mentionner la durée probable de l'interception.

4 – Les dispositions ci-après s'appliquent lorsqu'un État membre reçoit une notification en application des paragraphes 2 et 3.

a) Dès qu'elle a reçu les informations énumérées au paragraphe 3, l'autorité compétente de l'État membre notifié répond sans délai, et au plus tard dans les 96 heures, à l'État membre interceptant, en vue :

i) de permettre l'exécution ou la poursuite de l'interception. L'État membre notifié peut donner son consentement sous réserve de toutes conditions qui devraient être respectées dans une affaire nationale similaire ;
ii) d'exiger que l'interception ne soit pas effectuée ou soit interrompue lorsqu'elle ne serait pas autorisée en vertu du droit national de l'État membre notifié, ou pour les raisons mentionnées à l'article 2 de la Convention européenne d'entraide judiciaire. Lorsque l'État membre notifié impose cette exigence, il doit motiver sa décision par écrit ;
iii) d'exiger, dans les cas visés au point ii), que les données interceptées alors que la cible se trouvait sur son territoire ne puissent pas être utilisées ou ne puissent être utilisées que dans les conditions qu'il spécifie. L'État membre notifié informe l'État membre interceptant des motifs qui justifient lesdites conditions ;
iv) de demander, en accord avec l'État membre interceptant, que le délai initial de 96 heures soit prolongé d'une courte période qui ne peut dépasser 8 jours, afin d'accomplir les procédures internes requises par sa législation nationale. L'État membre notifié informe par écrit l'État membre interceptant des raisons qui, compte tenu de sa législation, justifient la demande de prolongation du délai.

b) Tant que l'État notifié n'a pas pris de décision conformément au point a), sous i) ou ii), l'État membre interceptant :
i) peut poursuivre l'interception ; et
ii) ne peut pas utiliser les données déjà interceptées, sauf
– s'il en a été convenu autrement entre les États membres concernés, ou
– pour prendre des mesures urgentes afin de prévenir un danger immédiat et sérieux pour la sécurité publique. L'État membre notifié est alors informé de l'utilisation de ces données et des motifs qui la justifient.

c) L'État membre notifié peut demander un résumé des faits et toute information complémentaire qui sont nécessaires pour lui permettre de décider si l'interception serait autorisée dans une affaire nationale similaire. Une telle demande n'affecte en rien l'application du point b), sauf accord contraire entre l'État membre notifié et l'État membre interceptant.

d) Les États membres prennent les mesures nécessaires pour assurer qu'une réponse est fournie dans le délai de 96 heures. À cette fin, ils désignent des points de contact, qui doivent être en service 24 heures sur 24, et les mentionnent dans leur déclaration conformément à l'article 24, paragraphe 1, point e).

5 – L'État membre notifié traite les informations communiquées en vertu du paragraphe 3 de manière confidentielle conformément à sa législation nationale.

6 – Lorsque l'État membre interceptant estime que les informations à communiquer en application du paragraphe 3 sont particulièrement sensibles, il peut les transmettre à l'autorité compétente par le biais d'une autorité spécifique lorsqu'il existe un accord bilatéral en ce sens entre les États membres concernés.

7 – Au moment de la notification visée à l'article 27, paragraphe 2, ou à tout autre moment ultérieur, un État membre peut déclarer qu'il ne sera pas né-

cessaire de lui fournir les informations relatives aux interceptions comme le prévoit le présent article.

Article 21
Prise en charge des coûts exposés par les exploitants des installations de télécommunication

Les frais exposés par les exploitants d'installations de télécommunications ou les fournisseurs de services du fait de l'exécution des demandes visées à l'article 18 sont à la charge de l'État membre requérant.

Article 22
Arrangements bilatéraux

Rien dans le présent titre n'empêche la conclusion d'accords bilatéraux ou multilatéraux entre États membres aux fins de faciliter l'exploitation de possibilités techniques présentes et futures en matière d'interception légale de télécommunications. (...)

Convention des Nations Unies contre la criminalité transnationale organisée – Résolution n° 25 du 15 novembre 2000

Article 20
Techniques d'enquête spéciales

1 – Si les principes fondamentaux de son système juridique national le permettent, chaque État Partie, compte tenu de ses possibilités et conformément aux conditions prescrites dans son droit interne, prend les mesures nécessaires pour permettre le recours approprié aux livraisons surveillées et, lorsqu'il le juge approprié, le recours à d'autres techniques d'enquête spéciales, telles que la surveillance électronique ou d'autres formes de surveillance et les opérations d'infiltration, par ses autorités compétentes sur son territoire en vue de combattre efficacement la criminalité organisée.

2 – Aux fins des enquêtes sur les infractions visées par la présente Convention, les États Parties sont encouragés à conclure, si nécessaire, des accords ou arrangements bilatéraux ou multilatéraux appropriés pour recourir aux techniques d'enquête spéciales dans le cadre de la coopération internationale. Ces accords ou arrangements sont conclus et appliqués dans le plein respect du principe de l'égalité souveraine des États et ils sont mis en œuvre dans le strict respect des dispositions qu'ils contiennent.

3 – En l'absence d'accords ou d'arrangements visés au paragraphe 2 du présent article, les décisions de recourir à des techniques d'enquête spéciales au niveau international sont prises au cas par cas et peuvent, si nécessaire, tenir compte d'ententes et d'arrangements financiers quant à l'exercice de leur compétence par les États Parties intéressés. (...)

Loi nº 2000-494 du 6 juin 2000 portant création d'une Commission nationale de déontologie de la sécurité

L'Assemblée nationale et le Sénat ont adopté,

Le Président de la République promulgue la loi dont la teneur suit :

Article 1er

La Commission nationale de déontologie de la sécurité, autorité administrative indépendante, est chargée, sans préjudice des prérogatives que la loi attribue, notamment en matière de direction et de contrôle de la police judiciaire, à l'autorité judiciaire, de veiller au respect de la déontologie par les personnes exerçant des activités de sécurité sur le territoire de la République.

Article 2

La Commission nationale de déontologie de la sécurité est composée de huit membres, nommés pour une durée de six ans non renouvelable :
– le président, nommé par décret du Président de la République ;
– un sénateur, désigné par le président du Sénat ;
– un député, désigné par le président de l'Assemblée nationale ;
– un conseiller d'État, désigné par le vice-président du Conseil d'État ;
– un magistrat hors hiérarchie de la Cour de cassation, désigné conjointement par le premier président de la Cour de cassation et par le procureur général près ladite cour ;
– un conseiller maître, désigné par le premier président de la Cour des comptes ;
– deux personnalités qualifiées désignées par les autres membres de la Commission nationale de déontologie de la sécurité.

La commission est renouvelée par moitié tous les trois ans.

La qualité de membre de la commission est incompatible avec l'exercice, à titre principal, d'activités dans le domaine de la sécurité.

Les parlementaires membres de la commission cessent d'y exercer leurs fonctions lorsqu'ils cessent d'appartenir à l'assemblée au titre de laquelle ils ont été désignés.

Si, en cours de mandat, un membre de la commission cesse d'exercer ses fonctions, le mandat de son successeur est limité à la période restant à courir. Par dérogation au premier alinéa, le mandat de ce dernier est renouvelable lorsqu'il a commencé moins de deux ans avant son échéance normale.

Lors de la première constitution de la Commission nationale de déontologie de la sécurité suivant l'entrée en vigueur de la présente loi, sont désignés par

tirage au sort quatre membres, à l'exclusion du président, dont les mandats prendront fin à l'issue d'un délai de trois ans.

Article 3

La commission établit son règlement intérieur,

En cas de partage des voix, celle du président est prépondérante.

Article 4

Toute personne qui a été victime ou témoin de faits dont elle estime qu'ils constituent un manquement aux règles de la déontologie, commis par une ou plusieurs des personnes mentionnés à l'article 1er, peut, par réclamation individuelle, demander que ces faits soient portés à la connaissance de la Commission nationale de déontologie de la sécurité. Ce droit appartient également aux ayants droit des victimes. Pour être recevable, la réclamation doit être transmise à la commission dans l'année qui suit les faits.

La réclamation est adressée à un député ou à un sénateur. Celui-ci la transmet à la commission si elle lui paraît entrer dans la compétence de cette instance et mériter l'intervention de cette dernière.

Le Premier ministre et les membres du Parlement peuvent, en outre, saisir de leur propre chef la commission de faits mentionnés au premier alinéa.

La commission ne peut être saisie par les parlementaires qui en sont membres.

Une réclamation portée devant la Commission nationale de déontologie de la sécurité n'interrompt pas les délais relatifs à la prescription des actions en matière civile et pénale et aux recours administratifs et contentieux.

Article 5

La commission recueille sur les faits portés à sa connaissance toute information utile.

Les autorités publiques doivent prendre toutes mesures pour faciliter la tâche de la commission. Elles communiquent à celle-ci, sur sa demande motivée, toutes informations et pièces utiles à l'exercice de sa mission telle qu'elle est définie à l'article 1er.

La commission peut demander dans les mêmes conditions aux ministres compétents de saisir les corps de contrôle en vue de faire des études, des vérifications ou des enquêtes relevant de leurs attributions. Les ministres informent la commission des suites données à ces demandes.

Les personnes privées exerçant des activités de sécurité sur le territoire de la République et leurs préposés communiquent à la commission, sur sa demande motivée, toutes informations et pièces utiles à l'exercice de sa mission.

Les agents publics ainsi que les dirigeants des personnes mentionnées au précédent alinéa et leurs préposés sont tenus de déférer aux convocations de la commission et de répondre à ses questions. Les convocations doivent mentionner l'objet de l'audition.

Les personnes convoquées par application de l'alinéa précédent peuvent se faire assister du conseil de leur choix. Un procès-verbal contradictoire de l'audition est dressé à la suite de celle-ci et remis à l'intéressé.

La commission peut consulter toute personne dont le concours lui paraît utile.

Le caractère secret des informations et pièces dont elle demande communication ne peut lui être opposé sauf en matière de secret de la défense nationale, la sûreté de l'État ou la politique extérieure, ainsi qu'en matière de secret médical et de secret professionnel applicable aux relations entre un avocat et son client.

Article 6

La commission peut charger un ou plusieurs de ses membres de procéder à des vérifications sur place.

Ces vérifications ne peuvent s'exercer que dans les lieux publics et les locaux professionnels, après un préavis adressé aux agents intéressés et aux personnes ayant autorité sur eux, ou pour le compte desquelles l'activité de sécurité en cause était exercée, afin de leur permettre d'être présents.

Toutefois, à titre exceptionnel, la commission peut décider de procéder à une vérification sans préavis si elle estime que la présence des agents intéressés ou des personnes ayant autorité sur eux n'est pas nécessaire.

Article 7

La commission adresse aux autorités publiques et aux dirigeants des personnes privées intéressés exerçant des activités de sécurité du territoire de la République tout avis ou recommandation visant à remédier aux manquements constatés ou à en prévenir le renouvellement.

Les mêmes autorités ou personnes concernées sont tenues, dans un délai fixé par la commission, de rendre compte à celle-ci de la suite donnée à ces avis ou recommandations.

En l'absence d'un tel compte rendu ou si elle estime, au vu du compte rendu qui lui est communiqué, que son avis ou sa recommandation n'a pas été suivi d'effet, la commission peut établir un rapport spécial qui est publié au Journal officiel de la République française.

Article 8

La commission ne peut intervenir dans une procédure engagée devant une juridiction. Elle ne peut remettre en cause le bien-fondé d'une décision juridictionnelle.

Lorsque la commission est saisie de faits donnant lieu à une enquête judiciaire ou pour lesquels une information judiciaire est ouverte ou des poursuites judiciaires sont en cours, elle doit recueillir l'accord préalable des juridictions saisies ou du procureur de la République, selon le cas, pour la mise en œuvre des dispositions de l'article 5 relatives à la communication de pièces et des dispositions de l'article 6.

Si la commission estime que les faits mentionnés dans la saisine laissent présumer l'existence d'une infraction pénale, elle les porte sans délai à la connaissance du procureur de la République, conformément aux dispositions de l'article 40 du code de procédure pénale.

Le procureur de la République informe la commission de la suite donnée aux transmissions faites en application de l'alinéa précédent.

Article 9

Sans préjudice des dispositions des articles 7 et 8, la commission porte sans délai à la connaissance des autorités ou des personnes investies du pouvoir disciplinaire les faits de nature à entraîner des poursuites disciplinaires. Ces autorités ou personnes informent la commission, dans le délai fixé par elle, de la suite donnée aux transmissions effectuées en application du présent article.

Article 10

La commission tient informé le parlementaire auteur de la saisine des suites données à celle-ci en application des articles 7 à 9.

Article 11

La Commission nationale de déontologie de la sécurité peut proposer au Gouvernement toute modification de la législation ou de la réglementation dans les domaines de sa compétence.

Article 12

La Commission nationale de déontologie de la sécurité remet chaque année au Président de la République et au Parlement un rapport sur les conditions d'exercice et les résultats de son activité. Ce rapport est rendu public.

Article 13

Les membres de la commission, ses agents, ainsi que les personnes que la commission consulte par application de l'avant-dernier alinéa de l'article 5, sont astreints au secret professionnel pour les faits, actes ou renseignements

dont ils ont pu avoir connaissance en raison de leurs fonctions, sous réserve des éléments nécessaires à l'établissement des rapports prévus aux articles 7 et 12.

Article 14

Les crédits nécessaires à la commission pour l'accomplissement de sa mission sont inscrits au budget des services du Premier ministre. Le président est ordonnateur des dépenses de la commission. Il nomme des agents et a autorité sur ses services.

Article 15

Est puni d'une amende de 50 000 F le fait de ne pas communiquer à la commission, dans les conditions prévues à l'article 5, les informations et pièces utiles à l'exercice de sa mission ou de ne pas déférer, dans les conditions prévues au même article, à ses convocations ou d'empêcher les membres de la commission d'accéder, dans les conditions prévues à l'article 6, aux locaux professionnels.

Les personnes physiques encourent également les peines complémentaires suivantes :
1° L'interdiction des droits civils, civiques et de famille, suivant les modalités prévues par l'article 131-26 du code pénal ;
2° L'affichage ou la diffusion de la décision prononcée, dans les conditions prévues à l'article 131-35 du code pénal.

Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues à l'article 121-1 du code pénal, du délit défini au premier alinéa. Les peines encourues par les personnes morales sont :
1° L'amende, suivant les modalités prévues par l'article 131-38 du code pénal ;
2° L'exclusion des marchés publics, suivant les modalités prévues par le 5° de l'article 131-39 du code pénal ;
3° L'affichage ou la diffusion de la décision prononcée, suivant les modalités prévues par le 9° de l'article 131-39 du code pénal.

Article 16

La présente loi est applicable en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis-et-Futuna, dans les Terres australes et antarctiques françaises et à Mayotte. Elle ne s'applique pas aux agents de la Polynésie française, du territoire des îles Wallis-et-Futuna, de la Nouvelle-Calédonie et des provinces de Nouvelle-Calédonie.

Proposition de loi tendant à la création de délégations parlementaires pour le renseignement, texte adopté par la commission de la défense nationale de l'Assemblée nationale

Article 1er

Il est inséré après l'article 6 *septies* de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires un article 6 *octies* ainsi rédigé :

« I – Il est institué, dans chacune des deux assemblées du Parlement, une délégation parlementaire pour le renseignement.

« II – Chaque délégation parlementaire pour le renseignement est composée :
– des présidents des commissions permanentes compétentes pour l'organisation générale de la défense, la politique extérieure et l'administration générale des territoires de la République et des collectivités locales, membres de droit ;
– d'un membre appartenant à la commission compétente pour l'organisation générale de la défense de chacun des groupes politiques de l'assemblée concernée, sur proposition de leurs présidents respectifs.

Le président de la commission permanente compétente pour l'organisation générale de la défense est président de droit de la délégation parlementaire pour le renseignement de son assemblée.

« III – La délégation de l'Assemblée nationale est désignée au début de chaque législature.

« La délégation du Sénat est désignée après chaque renouvellement partiel de cette assemblée.

« Le mandat des délégués prend fin avec leur mandat parlementaire, leur démission ou sur proposition motivée du Président de leur assemblée, après consultation du président du groupe concerné.

« Les délégués dont le mandat a pris fin en raison de l'expiration de leur mandat parlementaire, de leur démission ou d'une proposition motivée du Président de leur assemblée sont remplacés dans les conditions prévues au paragraphe II du présent article.

IV – Les délégations parlementaires pour le renseignement ont pour mission de suivre les activités des services visés à l'article 13 de l'ordonnance n° 59-147 du 7 janvier 1959 portant organisation générale de la défense, en examinant leur organisation et leurs missions générales, leurs compétences et leurs moyens, afin d'assurer, dans les conditions prévues au présent article, l'information de leur assemblée respective.

« Elles entendent les ministres ayant autorité sur ces services et les directeurs de ces services ou toute autre personne placée sous leur autorité et déléguée par eux.

« Elles entendent également toute personne susceptible de les éclairer et ne relevant pas de ces services.

« V – Les membres des délégations parlementaires pour le renseignement sont autorisés ès qualités à connaître d'informations classifiées dans le cadre de leur mandat.

« Ils sont astreints au respect du secret de la défense nationale protégé en application des articles 413-9 et suivants du code pénal pour les faits, actes ou renseignements dont ils ont pu avoir connaissance à raison de leur mandat.

« VI – Les travaux des délégations parlementaires pour le renseignement sont secrets, sous réserve des dispositions du paragraphe VII du présent article.

Dès leur désignation, les membres de chaque délégation prêtent serment dans les conditions fixées par le règlement intérieur prévu au paragraphe IX du présent article. Ils jurent et promettent de bien et fidèlement remplir leurs fonctions et de garder le secret des délibérations.

« Sera punie des peines prévues à l'article 226-13 du code pénal toute personne, qui, dans un délai de trente ans, divulguera ou publiera une information relative aux travaux d'une délégation parlementaire pour le renseignement sauf si un rapport publié par cette délégation en a préalablement fait état.

« VII – Chaque délégation pour le renseignement nomme un rapporteur spécial. Elle établit, au moins une fois par an, un rapport public de ses activités.

Ce rapport est transmis au Président de l'assemblée concernée qui le remet au Président de la République et au Premier ministre.

« VIII – La délégation de l'Assemblée nationale et celle du Sénat peuvent décider de tenir des réunions conjointes.

« IX – Chaque délégation parlementaire pour le renseignement établit son règlement intérieur. Celui – ci est soumis à l'approbation du Bureau de son assemblée. »

Article 2

À titre transitoire, chaque délégation parlementaire pour le renseignement est désignée dès la promulgation de la présente loi.

Questions parlementaires

Internet

Réseaux câblés et internet – directive européenne – application

34773 – 20 septembre 1999 – M. Olivier de Chazeaux appelle l'attention de M. le secrétaire d'État à l'industrie sur l'adoption d'une directive encourageant la concurrence dans le domaine des télécommunications locales et l'accès rapide à internet. Partant du constat que les mêmes opérateurs détiennent les réseaux téléphoniques et câblés, ce qui nuit à la concurrence, la directive instaure notamment une séparation juridique entre les deux activités (télévision par câble et télécommunications). Cette analyse est partagée par la Commission et le Parlement européen. Ces nouvelles règles doivent normalement encourager le développement de l'ensemble des services de télécommunications et par câble. Dans ces conditions et compte tenu de l'actuelle législation française en la matière, il lui demande les conséquences qu'il titre de l'adoption de cette directive.

Réponse – 5 juin 2000 – La directive 1999/64/CE du 23 juin 1999 est une directive de la Commission européenne prise en application de l'article 86 du Traité (compétence propre de la Commission en matière de concurrence). Aux termes de son article 1er, « chaque État membre veille à ce que tout organisme de télécommunications ne fasse pas appel, pour l'exploitation de son réseau câblé de télévision, à la même entité juridique que pour son réseau de télécommunications lorsque l'organisme en question : a) est contrôlé par cet État membre ou bénéficie de droits spéciaux ; b) déteint une position dominante dans une partie substantielle du marché commun pour fourniture de réseaux de télécommunications publics et de services publics de téléphonie vocale, et, c) exploite un réseau câblé de télévision établi en vertu de droits spéciaux ou exclusifs dans la même zone géographique ». Cette directive est d'application directe dans tous les États membres et n'entraîne pas de me-

sure de transposition. Il appartient donc aux États membres de prendre directement les mesures individuelles qui s'imposent. Au cas particulier de la France, la distinction juridique concernant les activités de France Télécom est bien réalisée : France Télécom dont le capital est détenu à 98 % par COGECOM et TDF. Conformément aux dispositions de l'article 3 de cette directive, le ministère de l'économie, des finances et de l'industrie prépare la réponse des autorités françaises à la Commission lui permettant de constater que les dispositions de l'article 1er sont respectées. Par ailleurs, les autres réseaux câbles possédés par France Télécom sont commercialement exploités par des sociétés distinctes de l'opérateur public (Lyonnaise Câble, Paris RV Câble et Numéric Câble).

Commerce électronique – transactions – contrôle

26507 – 8 mars 1999 – M. Bernard Accoyer appelle l'attention de M. le secrétaire d'État à l'industrie sur les dérives liées à la commercialisation sur internet. En effet, il apparaît que ce nouveau mode de communication est utilisé pour commercialiser en toute impunité des produits illégaux (stupéfiants, annonces à caractère déviant, pédophilie...) et même des produits pour lesquels des garanties sont édictées, tels, par exemple, certains médicaments. Il lui demande de bien vouloir lui indiquer les mesures qu'il compte prendre afin de remédier à ce type de commercialisation illégale. – Question transmise à Mme la secrétaire d'État aux petites et moyennes entreprises, au commerce, à l'artisanat et à la consommation.

Réponse – 8 mai 2000 – Le droit du commerce électronique est en cours de définition. Le Conseil a approuvé une position commune sur le projet de directive européenne relative à la société de l'information. Ce texte sera transposé en droit interne par la loi sur la société de l'information. Ces différents textes visent à protéger les consommateurs sur la base de la législation en matière de vente à distance ou de démarchage en vigueur dans le pays d'établissement du vendeur ou du prestataire de services. Les droits du consommateur en situation d'achat à distance ou à domicile font d'ores et déjà l'objet d'une harmonisation entre les États et l'Union européenne. Cependant, le principe de l'application du droit de l'État d'origine de l'offre de vente comportera des dérogations pour les activités dont la réglementation ne serait pas harmonisée ou qui ne donneraient pas lieu à une reconnaissance mutuelle si elle porte atteinte à l'intérêt général. Par ailleurs, un dispositif devra être mis en place afin d'éviter qu'un prestataire ne s'établisse sur le territoire d'un État membre différent de celui auquel les services sont destinés, dans le seul but de se soustraire à la réglementation de cet État (dispositif anticontournement). En outre, la renégociation des conventions de Bruxelles et de Rome est en cours. Elle devrait permettre de déterminer plus assurément le droit et la juridiction applicables qui devraient être ceux du pays du consommateur. Pour ce qui est des activités illégales sur l'internet, il convient de réaliser une plus grande transparence du réseau en aménageant la conversation des données de connexion des utilisateurs. Chaque connexion effectuée par le canal d'un fournisseur d'accès engendre des don-

nées susceptibles d'être conservées chez le fournisseur d'accès ou sur les serveurs des sites consultés par l'internaute. Ainsi, l'identité de l'abonné, l'heure du début et de fin de communication, mais aussi les différents sites fréquentés peuvent techniquement être répertoriés. Ces données, usuellement utilisées pour facturer les communications, peuvent être rendues accessibles dans le cadre d'une enquête judiciaire pour rechercher éventuellement l'auteur d'une infraction commise au moyen du réseau. La conservation des données appelle la définition de spécifications techniques afin d'en garantir la fiabilité. Elle doit surtout s'effectuer dans des conditions respectueuses des libertés publiques, en particulier sur le plan de la protection de la vie privée. Il appartient donc à la loi de fixer les limites quant à la nature des informations conservées et la durée de leur archivage. Les conditions d'accès de l'autorité judiciaire aux données de connexion seront celles définies par le droit commun.

Internet – réglementation internationale

50977 – 18 septembre 2000 – M. André Aschieri attire l'attention de M^me^ le garde des sceaux, ministre de la justice, sur l'actuelle absence de standardisation des normes juridiques internationales spécifiques à internet et plus particulièrement liées aux échanges sur le web. La situation actuelle présente l'inconvénient majeur de freiner leur développement. Aujourd'hui, chaque pays tend à instaurer sa propre législation nationale, tant pour réglementer ces échanges que pour proposer une taxation du commerce électronique. La nature même d'internet tend vers une unification des pratiques juridiques. Il souhaite donc savoir si, tout en préservant la gratuité et l'échange qui caractérise ce média, elle entend prendre des initiatives afin de participer à l'élaboration des règles juridiques internationales et d'éviter de voir ainsi s'imposer d'autres modèles juridiques.

Réponse – 4 décembre 2000 – Le garde des sceaux, ministre de la justice, fait connaître à l'honorable parlementaire que sa question a retenu toute son attention. Soucieux de prendre en compte le développement de l'internet dans toutes ses spécificités, le gouvernement français s'est impliqué activement dès l'origine dans les différentes négociations internationales. De nombreux aspects de la société mondiale de l'information sont abordés, en particulier le commerce électronique (directive sur le commerce électronique du 8 juin 2000), la signature électronique (loi reconnaissant valeur de preuve à la signature électronique du 13 mars 2000). Dans ce domaine, où la France est en avance sur la plupart de ses partenaires, le décret d'application est en cours d'élaboration et a fait l'objet d'une consultation publique qui s'est achevée le 15 septembre. La France prend également une part active à la phase finale de la négociation de la convention du Conseil de l'Europe sur la cybercriminalité dont la négociation doit aboutir d'ici la fin de l'année 2000. En fonction des résultats de ces négociations et sur la base des propositions que doit faire la Commission européenne, la France et ses partenaires européens envisageront l'utilité de l'adoption d'un instrument spécifique à l'Union européenne en la matière, conformément aux discussions du Conseil justice et

affaires intérieures du 28 juillet 2000. Dans ce même domaine, la France a organisé en mai dernier, dans le cadre du G8, une rencontre internationale à Paris entre acteurs privés du monde de l'internet et pouvoirs publics. Cette conférence a permis, pour la première fois, aux entreprises privées de reconnaître les difficultés qu'elles rencontraient et de les exposer aux autorités publiques, permettant à celles – ci d'être informées des besoins et d'envisager les mesures nécessaires pour assurer un développement fiable de l'internet. Cette réunion a été suivie d'experts à Berlin en octobre 2000 avant une rencontre au Japon en 2001, échéance que le Gouvernement prépare en collaboration avec ses partenaires. Par ailleurs, sur le plan national, la France, engagée depuis plus de trois ans dans l'élaboration de règles destinées à préserver à la fois le caractère spécifique de l'internet, son développement et à assurer la sécurité des échanges qui s'y déroulent, veille à ce que le projet de loi sur la société de l'information, en phase finale d'élaboration, prenne en compte les différentes directives européennes déjà entrées en vigueur ainsi que les instruments internationaux en cours d'élaboration.

Criminalité – lutte – prévention

Internet – infractions – lutte et prévention

42302 – 28 février 2000 – M. Michel Hunault attire l'attention de M. le ministre de l'économie, des finances et de l'industrie sur la vulnérabilité des sites présents sur internet. Alors que l'usage internet banalise dans les rapports entre particuliers, entre entreprises et consommateurs et au sein même des administrations, il lui demande quelles mesures a prises le Gouvernement pour lutter contre la délinquance visant à perturber le fonctionnement des sites, le « vandalisme électronique » ainsi que la prise illicite d'informations par les cybercriminels.

Réponse – 10 juillet 2000 – La sécurité sur internet et la mise en place d'un cadre de confiance pour les services de la société de l'information passent par l'adaptation de notre cadre juridique à la société de l'information. Cette adaptation, annoncée en août dernier par le Premier ministre, est en cours. Le Gouvernement présentera à l'automne un projet de loi sur la société de l'information articulé autour de trois orientations : la liberté de communication, qui doit être au cœur de la société de l'information ; l'accès du plus grand nombre aux réseaux de la société de l'information ; la sécurité de l'information ; la sécurité et la loyauté des transactions en ligne, afin de renforcer la confiance des utilisateurs et de promouvoir la transparence sur les réseaux. La garantie de la confidentialité des informations échangées sur des réseaux ouverts comme internet constitue l'un des éléments essentiels de cette sécurité. La libération de l'utilisation de la cryptologie est à cet égard un élément important. Elle permettra aux entreprises et aux particuliers d'utiliser des outils permettant de protéger efficacement l'information circulant sur internet. Cette libéralisation a été entamée en février 1998, par les textes d'application de la loi de réglementation des télécommunications

(LRT) de 1996. Une nouvelle étape a été franchie en mars 1999 par le relèvement du seuil des outils dispensés de toute formalité de 40 bits à 128 bits. La liberté d'utilisation des moyens de cryptologie sera bientôt rendue totale par une modification de la LRT que proposera le Gouvernement. Par ailleurs, à travers ses programmes d'aide à la recherche et développement, notamment le programme Société de l'information, le secrétariat d'État à l'industrie soutient activement le développement d'une offre de produits de sécurité des technologies de l'information (à titre d'exemple, le développement de lecteurs de cartes à puce sécurisés à bas coût permettant l'utilisation des cartes à puce bancaires pour effectuer des paiements sur internet en toute sécurité). Ces actions sont menées en parfaite cohérence avec celles conduites par le service central de la sécurité des systèmes d'information qui, placé auprès du Premier ministre, travaille notamment dans le domaine de l'évaluation du niveau de qualité de ces produits. Le Gouvernement a annoncé que le SCSSI, intégré au secrétariat général de la défense nationale depuis le 1er janvier 1999, serait transformé au cours de l'année 2000 en direction plein exercice du SGDN, chargé de la sécurité des systèmes d'information au niveau interministériel. Cette décision marque à la fois un changement d'échelle dans les moyens dont le gouvernement souhaite se doter dans ce domaine et la volonté d'assurer une meilleure coordination des efforts de l'État. Enfin un office central de lutte contre la criminalité liée aux technologies de l'information et de la communication a été crée le 15 mai dernier au sein de la direction centrale de la police judiciaire (DCPJ) du ministère de l'intérieur, sur le modèle des huit offices centraux déjà existants. Cet office central sera le point de contact pour la France dans un réseau international de police judiciaire et de justice pénale, dont les actions seront ainsi coordonnées à l'échelon central. Il a pour vocation d'élaborer les outils nécessaires à la répression de la criminalité des technologies numériques.

Internet – infractions – lutte et prévention

44469 – 3 avril 2000 – M. Guy Lengagne appelle l'attention de Mme la ministre de la culture et de la communication au sujet des problèmes juridiques liés au respect de la loi sur les réseaux internet. Il est indéniable que le réseau internet est à l'heure actuelle un formidable espace de liberté d'expression et de communication. Encore faut-il ne pas profiter de cette liberté, qui est un des principes fondamentaux d'un État de droit, pour commettre des infractions ou obtenir un profit illicite. En ce sens, les utilisateurs d'un site internet doivent être protégés. Un contrôle, à l'émission du contenu d'internet, soulève des obstacles difficilement surmontables pour une autorité publique. Toutefois, face au risque d'infractions liées aux contenus circulant sur le réseau, un arsenal juridique important est disponible, de par la protection des droits d'auteur, du consommateur, de l'individu et de sa vie privée, des mineurs, et de par la répression des actes racistes ou xénophobes par la loi no 90-615 du 13 juillet 1990. Le dispositif textuel est donc suffisant, en l'état, pour sanctionner la plupart des infractions concernant la protection des personnes, des consommateurs et des données. Mais la spécificité du réseau internet suscite des obstacles matériels à sa mise en œuvre effective. Tout

d'abord, le caractère fugace des contenus véhiculés par internet, notamment l'aisance avec laquelle un site peut être supprimé ou déplacé, ou son contenu modifié, rend l'enquête pénale et l'application de certains textes difficiles, car la réalité même de l'infraction reste délicate à établir. La rapidité d'évolution des techniques est d'autre part une source de difficultés supplémentaires. Enfin, des pressions existent, dans le cadre des relations internationales, pour modifier l'état actuel du droit : ainsi, en matière de protection des consommateurs, le risque est réel de voir se substituer au droit français, considéré aujourd'hui comme applicable, le seul droit du pays du vendeur de produit ou du service offerts sur internet, car des intérêts extérieurs à la France y incitent fortement. Il lui demande donc de bien vouloir lui faire connaître les intentions du Gouvernement en la matière.

Réponse – 28 août 2000 – Comme le souligne l'honorable parlementaire, l'internet n'est pas un espace de non-droit et le droit positif est à même d'appréhender le réseau. Il est toutefois susceptible de se heurter à des difficultés d'application face au caractère transnational du réseau. L'orientation générale des instruments de droit international privé en vigueur au sein de l'Union européenne contribue dans ce contexte à garantir aux consommateurs la possibilité de saisir des juridictions appropiées à leur situation et de les faire bénéficier de l'application de la loi qui leur est la plus favorable. La convention de Rome du 19 juin 1980 sur la loi applicable aux obligations contractuelles comporte à son article 5 des dispositions protectrices du consommateur visant à lui appliquer la loi du pays dans lequel il a sa résidence habituelle. Le Gouvernement a ainsi rappelé dans son document d'orientation sur le cadre juridique de la société de l'information soumis à consultation publique à l'automne 1999 que le consommateur concluant un contrat en ligne ne peut être privé de la protection que lui assurent les dispositions protectrices de la loi du pays de sa résidence habituelle. Cette position a été traduite dans la proposition de la directive relative à certains aspects juridiques des services de la société de l'information que le consommateur, et notamment de commerce électronique, adoptée par le Parlement européen le 3 mai 2000. Cette dernière prévoit à son article 1er qu'elle n'établit pas de règles additionnelles du droit international de droit privé et ne traite pas de la compétence des juridictions. Les dispositions de l'article 3 relatives au marché intérieur ne sont en outre pas applicables aux obligations contractuelles concernant les contrats conclus pas les consommateurs. Cette directive sera transposée dans le cadre du projet de loi pour la société de l'information que prépare le Gouvernement.

Internet – criminalité – lutte et prévention

49092 – 17 juillet 2000 – M. Armand Jung attire l'attention de M. le ministre de l'intérieur sur les propositions de lutte contre la cybercriminalité. À l'occasion de la récente conférence du G 8 sur le thème de la sécurité et de la confiance dans le cyberespace, la France a annoncé les principes de son action pour lutter contre les nouvelles formes de criminalité sur internet. En

conséquence, il lui demande de bien vouloir détailler les propositions françaises dans ce domaine.

Réponse – 9 octobre 2000 – La lutte contre la cybercriminalité est une préoccupation majeure partagée par de nombreux pays. Elle vise, à la fois, à limiter le recours aux technologies de l'information et de la communication facilitant l'action de groupes criminels (pédophilie, blanchiment), à contribuer à la sécurité des industriels, opérateurs ou fournisseurs de services concernés, et à protéger les libertés individuelles et la vie privée des utilisateurs. Cette criminalité occulte ne peut être combattue que si les pouvoirs publics disposent préalablement des moyens humains et techniques nécessaires pour la détecter. Dans le domaine de la prévention, le Gouvernement fait porter ses efforts sur la formation des utilisateurs de l'internet. Les décisions prises par le Comité interministériel pour la société de l'information du 10 juillet 2000 visent à faciliter l'accès de l'internet à tous en généralisant la formation à l'informatique, au multimédia et à l'internet dans l'éducation, l'apprentissage et la formation professionnelle. Il s'agit notamment de sensibiliser les internautes aux obligations légales liées aux réseaux d'information et de les responsabiliser. Vis-à-vis des industriels, des opérateurs de télécommunications et des prestataires techniques de l'internet, le Gouvernement préconise la corégulation sur la base de règles fixées en commun. Mais le développement d'internet et du commerce électronique génère de multiples infractions pénales qui nécessitent une action répressive fondée sur de nouvelles mesures juridiques et la mise en place d'un nouveau service de police spécialisé. Outre la loi sur la signature électronique votée par le Parlement au mois de mars 2000, un projet de loi sur la société de l'information est en cours d'élaboration au ministère de la justice. Un chapitre important de ce texte sera consacré à la criminalité informatique. Le projet de loi devrait être présenté au Parlement dès le printemps prochain. L'office central de lutte contre les infractions liées aux technologies de l'information et de la communication a été créé par décret interministériel du 15 mai 2000 Cet office interministériel, rattaché à la direction centrale de la police judiciaire, est composé de policiers spécialisés et sera prochainement renforcé par d'autres fonctionnaires de police, des gendarmes, des douaniers et des ingénieurs spécialisés dans les réseaux de communication. Enfin, en matière de coopération internationale, le Gouvernement entend poursuivre une politique active de lutte contre la cybercriminalité qui revêt un caractère mondial, tant au niveau du G8 que du Conseil de l'Europe ou de l'Union européenne. La conférence du G8 sur « la sécurité et la confiance dans le cyberespace », qui s'est tenue à Paris du 15 au 17 mai 2000, a réuni les spécialistes du secteur privé et du secteur public des huit pays les plus développés. Ce dialogue sera poursuivi au plan national dans chaque État membre. Au sein du Conseil de l'Europe, le projet de « convention sur la criminalité dans le cyberspace » est très avancé et les travaux du comité d'experts devraient être terminés pour la fin de l'an 2000. Par ailleurs, dans le cadre de la présidence française de l'Union européenne, la France demande l'extension de la compétence d'Europol à la criminalité informatique et organise en novembre prochain un séminaire européen consacré à la cybercriminalité. Ces

rencontres d'enquêteurs spécialisés en criminalité informatique permettront un échange direct d'expériences et de compétences particulières entre spécialistes du réseau internet et contribueront ainsi à améliorer le niveau technique de maîtrise et d'investigation des enquêteurs européens. L'objectif est d'établir un guide méthodologique pratique d'enquête judiciaire en milieu informatique. La création dans les États membres de structures centrales nationales spécialisées, points de contact pour la coopération internationale, est privilégiée afin d'assurer une meilleure centralisation et coordination des informations et des actions de lutte contre la cybercriminalité. Cette généralisation du dispositif à l'ensemble des pays de l'Union européenne permettait d'étendre le réseau des points de contact nationaux (24 heures sur 24 et 7 jours sur 7) mis en place dans le cadre du sous-groupe « criminalité de haute technologie » G8.

Internet – infractions – lutte et prévention

46762.– 22 mai 2000 – M. Jean-Luc Warsmann attire l'attention de M. le ministre de l'intérieur au sujet des moyens de lutte et des données statistiques sur la criminalité liée aux nouvelles technologies de l'information et des communications. La cybercriminalité couvre deux catégories de phénomènes : une criminalité spécifique aux technologies de l'information (atteinte au système de traitement automatisé de données par intrusion volontaire dans le serveur d'une entreprise) et une criminalité facilitée par les technologies de l'information (escroquerie au moyen de cartes bancaires). Ces nouvelles pratiques criminelles nécessitent la création de nouveaux moyens de lutte, mais aussi la définition de nouvelles approches méthodologiques permettant d'appréhender et d'évaluer l'ampleur du phénomène dans toute sa diversité. Aussi, il souhaiterait connaître les études et les projets du Gouvernement sur ces phénomènes de cybercriminalité.

Réponse – 6 novembre 2000 – L'office de lutte contre les infractions liées aux technologies de l'information et de la communication a été créé par le décret du 15 mai 2000. Situé au ministère de l'intérieur au sein de la direction générale de la police nationale à la direction centrale de la police judiciaire, il vient enrichir le dispositif de lutte existant contre la cybercriminalité. Il se substitue à la brigade de répression de la criminalité informatique, créée en 1994 par la direction centrale de la police judiciaire, qui intégrera le nouvel office Les moyens de lutte engagés pour lutter contre ces nouvelles pratiques criminelles, communément appelées « cybercriminalité » pourront être ainsi développés sur le modèle déjà existant, notamment par des formations de haut niveau dispensées aux enquêteurs spécialisés et la mise à disposition d'un matériel informatique performant en terme de recherche et d'investigations. Par ailleurs, des rencontres internationales entre spécialistes des secteurs privés (fournisseurs d'accès à interne) et publics ont déjà eu lieu dans le cadre des activités du G8 (conférence de Paris du mois d'avril 2000) et se poursuivront dans le cadre de la Présidence française de l'Union européenne par un séminaire organisé

par la direction centrale de la police judiciaire devant se dérouler au Futuroscope de Poitiers du 13 au 17 novembre 2000. Ces rencontres permettent un échange direct entre spécialistes du réseau internet et contribuent à améliorer le niveau technique de maîtrise et d'investigation des enquêteurs spécialisés de ce nouvel office. Enfin, les experts français vont assurer, au niveau international, le suivi des travaux lancés dans différentes enceintes pour améliorer, par des outils juridiques adaptés, l'efficacité de la lutte contre les délits véhiculés par ces nouveaux outils technologiques. La sensibilisation des opérateurs de télécommunications, des organismes bancaires ou des prestations techniques par le ministère de l'intérieur va se poursuivre afin que le renforcement de la sécurité des utilisateurs des nouvelles technologies de l'information et de la communication aboutisse à une limitation de ce type d'infraction. En ce qui concerne la définition de nouvelles approches permettant d'évaluer l'ampleur du phénomène de la cybercriminalité, une étude est en cours pour adapter les outils statistiques de la police nationale au recueil des informations concernant la criminalité informatique, en évitant à la fois le double comptage des infractions – celles-ci étant souvent facilitées par le recours aux nouvelles technologies – et une charge de travail de saisie excessive pour les enquêteurs concernés. La modification de l'état statistique 4001, utilisé depuis vingt-six ans par les services de police et de gendarmerie, paraît difficilement envisageable dans la mesure où cet outil vise à une approche générale de la criminalité principalement axée sur la délinquance de voie publique, et qu'une telle modification ne permettrait plus de procéder à des comparaisons sérielles dans le temps. Par ailleurs, cet outil statistique destiné à la connaissance de l'action des services de police et de gendarmerie dans la lutte contre la délinquance locale ou territoriale n'est pas suffisant pour mesurer la cybercriminalité, par essence internationale. Toutefois, l'office central de lutte contre les infractions liées aux technologies de l'information et de la communication aura pour mission comme tous les autres offices centraux, de créer et de gérer des outils de collecte et d'analyse d'information sur les phénomènes à combattre.

Internet – sites néonazis – lutte et prévention

49037 – 17 juillet 2000 – M. Armand JUNG attire l'attention de M^me^ la garde des sceaux, ministre de la justice, sur le problème des sites d'enchères néonazis sur internet. Les sites faisant la promotion de la période néonazie ont investi l'internet et sont accessibles à tous les internautes à travers le monde. Une sorte de « cyber-impunité » semble s'installer au nom de la libre expression Cependant plusieurs associations ont réagi face à cela et la justice française a jugé de façon stricte cette affaire en imposant des barrières à la publication de certains sites. Pour autant tout n'est pas réglé. En conséquence, il lui demande si des mesures concrètes vont être envisagées pour interdire la mise en réseau de tels sites.

Réponse – 23 octobre 2000 – Le garde des sceaux, ministre de la justice, souhaite tout d'abord rappeler à l'honorable parlementaire que le Gouvernement a affirmé, publiquement et à de nombreuses reprises, sa ferme volonté

de combattre l'ensemble des manifestations à caractère raciste ou révisionniste, quels que soient le lieu et le support leur expression. Ainsi, en ce qui concerne le cas spécifique de la lutte contre le racisme ou le révisionnisme sur les réseaux téléinformatiques de type internet, il convient d'infirmer l'affirmation trop souvent entendre selon laquelle il existerait un vide juridique en la matière. Le droit positif français permet en effet de réprimer la diffusion de tout discours raciste ou révisionniste, par quelque moyen que ce soit et quel qu'en soit le support, pour reprendre les termes mêmes du code pénal. La difficulté majeure de l'action répressive en ce domaine est induite le plus souvent par la localisation des sites à caractère raciste ou révisionniste consultables par les internautes français dans des pays ou ces formes d'expression sont tolérées voire protégées par des textes à valeur constitutionnelle garantissant la liberté d'expression. Le renforcement de la coopération internationale, possible avec les États, appartement notamment à l'Union européenne, partageant les mêmes normes et les mêmes objectifs que notre pays en ce domaine, se révèle alors délicat. Les obstacles tenant à un insuffisant développement de l'entraide judiciaire internationale n'ont cependant pas amené le Gouvernement à renoncer à son objectif publiquement affiché de lutte contre toutes les formes de racisme et de révisionnisme. C'est ainsi que, par un décret en date du 15 mai 2000, a été créé un nouvel office central, l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. Cette structure spécialisée rassemblant des officiers de police judiciaire formés aux nouvelles technologies et disposant des matériels les plus perfectionnés permettra à l'institution judiciaire d'accentuer l'efficacité de son activité répressive à l'encontre des créateurs de sites racistes ou révisionnistes.

Nouvelles technologies

Concurrence – dégroupage – perspectives

39055 – 20 décembre 1999 – M. André Adchieri attire l'attention de M. le secrétaire d'État à l'industrie sur le dégroupage qui est une technique permettant aux opérateurs concurrents d'accéder à la prise téléphonique de France Télécom. En effet, l'autorité de réglementation des télécoms vient de procéder à une large consultation des acteurs du domaine sur le dégroupage. L'argumentation en faveur du dégroupage repose sur le fait qu'il accélérera l'émergence de la concurrence et la baisse des prix. Ce point de vue pourrait aussi aboutir à un écrémage du marché empêchant le citoyen s'installant dans une zone rurale ou montagneuse, de bénéficier des services existants à des prix accessibles. Il souhaite connaître sa position sur ce sujet.

Réponse – 5 juin 2000 – Le développement et le déploiement sur le territoire français des accès à internet à haut débit pour les entreprises et les particuliers, à travers les réseaux existants et de nouvelles infrastructures, constituent une des priorités du Gouvernement comme en témoigne le document d'orientation sur l'adaptation du cadre juridique de la société de l'informa-

tion rendu public le 5 octobre 1999. Ainsi, le déploiement de la technologie ADSL par France Télécom qui devrait être suivi par d'autres opérateurs grâce au dégroupage de la boucle locale de l'opérateur historique, permettra un accès à haut débit à l'Internet sur une grande partie du territoire français via l'utilisation des lignes téléphoniques classiques. La technologie ADSL ne peut cependant être généralisée à l'ensemble du territoire en raison de contraintes techniques : la ligne téléphonique ne doit pas excéder quelques kilomètres depuis le central téléphonique, au-delà le fonctionnement et la qualité de service ne sont plus garantis. L'émergence d'alternatives techniques actuellement à l'étude, notamment l'utilisation de technologies satellitaires (satellite géostationnaire ou constellation de satellites en orbite basse), laisse entrevoir la possibilité d'apporter des solutions plus adaptées aux zones géographiques moins denses. Par exemple, le projet de constellation de satellites Skybridge, auquel le secrétaire d'État à l'industrie vient d'accorder une autorisation pour fournir des services de télécommunications en France, devrait être opérationnel à partir de 2002. Les offres commerciales envisagées par Skybridge devraient permettre de fournir un accès forfaitaire à haut débit à l'internet à des tarifs voisins de ceux des offres équivalentes sur les réseaux câblés ou à base de technologie ADSL, soit environ 300 francs par mois. De même, la boucle locale radio (BLR), qui permet de raccorder les abonnés par voie hertzienne, constitue une technique fiable et peu onéreuse (par rapport au coût de la pose de fibre optique). Le Gouvernement a donc lancé le 30 novembre 1999 trois appels à candidatures pour des licences de BLR. Les vingt-huit candidatures qui ont été déposées auprès de l'Autorité de régulation des télécommunications au 31 janvier 2000 laissent penser que, dans chaque région française, quatre opérateurs de télécommunications investiront dans la boucle locale radio. Les autorisations et les fréquences correspondantes seront attribuées à partir du quatrième trimestre 2000. Le Gouvernement considère que la couverture du territoire français par des services de télécommunications à haut débit se fera grâce à l'utilisation de toutes les technologies disponibles dont l'intérêt technique et économique peut être variable selon les zones à couvrir.

Concurrence – dégroupage – perspectives

48683 – 10 juillet 2000 – M. Georges Sarre appelle l'attention de M. le secrétaire d'État à l'industrie sur l'ouverture envisagée par le Gouvernement, aux opérateurs privés, des infrastructures de France Télécom permettant d'accéder à l'abonné, plus couramment appelée dégroupage. Il rappelle que le dégroupage revient à mettre le réseau public à la disposition d'opérateurs privés, les dispensant par là même de réaliser des investissements dans d'autres technologies alternatives et innovantes, comme les réseaux câblés ou la boucle locale radio. Il insiste sur le fait que des opérateurs privilégiant les contenus pourraient être amenés à utiliser les infrastructures publiques pour développer leur offre. Il s'interroge également sur le changement de voie apparemment intervenu pour procéder à cette intensification de la concurrence, le Gouvernement ayant un temps envisagé de recourir à la voie législative dans le cadre de la discussion du projet de loi sur les « nouvelles

régulations économiques », alors qu'il semble envisager depuis de recourir au décret. Il considère qu'une telle réforme, dont il conteste l'orientation, trouverait logiquement sa place dans le cadre d'une délibération parlementaire, s'agissant d'un réseau mis en place par l'opérateur public, et financé par la collectivité. C'est pourquoi, il lui demande quelle décision il entend prendre au sujet du dégroupage, et quelle voie, réglementaire ou législative, il entend emprunter, sachant que la seconde lui paraît préférable. Il souhaite également connaître les obligations en termes de redevance d'utilisation que le Gouvernement à l'intention de mettre en place pour garantir une juste rémunération de ses infrastructures à l'opérateur public France Télécom.

Réponse. – 11 septembre 2000 – Lors du comité interministériel sur la société de l'information du 10 juillet 2000, le Premier ministre a rappelé l'importance qu'il attache à la généralisation rapide de l'offre d'accès à haut débit à internet. Il s'agit en effet d'une condition importante du développement de l'accès à internet en France et donc de sa démocratisation. Plusieurs technologies apparaissent aujourd'hui envisageables pour fournir de tels accès (boucle locale radio-électrique, câble, satellite, xDSL, etc...), et le Gouvernement s'emploie à lever les obstacles à leur développement. Les technologies xDSL, qui permettent de fournir des accès à internet à haut débit à partir des lignes téléphoniques existantes, s'avèrent particulièrement prometteuses pour ce qui est de la clientèle grand public. Aussi, le Gouvernement souhaite que les services utilisant ces technologies puissent se développer dans un cadre permettant une concurrence effective. Étant donné l'impossibilité de dupliquer à court terme les lignes téléphoniques du réseau de France Télécom, une concurrence sur les services utilisant les technologies xDSL n'est possible que si les opérateurs concurrents ont accès aux lignes téléphoniques existantes pour fournir leurs services (dégroupage de la boucle locale). Lors du comité interministériel sur la société de l'information du 10 juillet 2000, le Premier ministre a indiqué que le dégroupage serait mis en œuvre par la voie réglementaire. Le décret sur le dégroupage de la boucle locale devrait être adopté avant la fin de l'été pour entrer en application le 1er janvier 2001. Il garantira à l'exploitant public une juste rémunération pour l'utilisation des infrastructures qu'il a installées. Il est en effet important que la tarification du dégroupage de la boucle locale ne soit pas trop basse afin de ne pas décourager l'investissement dans de nouvelles infrastructures là où il s'avérerait pertinent. Par ailleurs, la Commission européenne a proposé, le 12 juillet 2000, un projet de règlement relatif au dégroupage de la boucle locale. Ce règlement, dont l'adoption rapide constitue un des objectifs de la présidence française dans le domaine des télécommunications, permettrait aux opérateurs français, et notamment France Télécom, de bénéficier du dégroupage de la boucle locale dans l'ensemble des pays de l'Union européenne.

Télécommunications

Annuaire universel

22293 – 13 juillet 2000 – M. François Autain attire l'attention de M. le secrétaire d'État à l'industrie sur « l'annuaire universel », visé par la loi nº 96-659 de réglementation des télécommunications. En effet, cette loi a créé, dans le code des postes et télécommunications, un article L. 35-4 qui prévoit la mise en place d'un annuaire universel regroupant la liste de l'ensemble des abonnés au téléphone, et ce quel que soit l'opérateur auprès duquel ils sont abonnés. Cet « annuaire universel » doit être tenu et édité par un organisme « juridiquement distinct des entreprises offrant des biens ou services de télécommunication » et créé par décret en conseil d'État. Or, à ce jour, cet organisme n'a toujours pas été créé. Il n'existe donc pas d'annuaire universel. Aussi, les abonnés au téléphone qui ne sont pas clients de l'ancien opérateur public ne figurent pas dans l'annuaire édité par France Télécom. Cette situation s'avère préjudiciable pour les abonnés des sociétés concurrentes de l'ancien opérateur public. En conséquence, il lui demande si le Gouvernement entend soumettre au Conseil d'État un projet de décret créant cet organisme. Dans l'affirmative, un calendrier est-il arrêté pour l'adoption du décret d'application visé à l'article L. 35-4 ? Quel statut, quelle composition et quelles conditions de fonctionnement sont envisagés pour cet organisme ? Quels moyens seront mis à sa disposition et comment son financement sera-t-il assuré ?

Réponse – 7 septembre 2000 – La multiplication des opérateurs liée à la libéralisation du marché des télécommunications, ainsi que l'essor très rapide de la téléphonie mobile ont fait apparaître la nécessité de mettre à la disposition des utilisateurs un annuaire universel rassemblant l'ensemble des numéros des abonnés quel que soit l'opérateur dont ils dépendent, qu'il s'agisse de téléphone fixe ou mobile. Les dispositions de l'article L. 35-4 du code des postes et télécommunications adoptées à cette fin ont pris en compte les réticences exprimées par les opérateurs entrants de transmettre leur liste d'abonnés à France Télécom en vue de l'édition de l'annuaire universel. Le législateur a ainsi prévu la création d'un organisme indépendant servant d'interface entre les opérateurs et les éditeurs d'annuaires, chargé de rassembler toutes les listes d'abonnés pour créer une liste universelle et de fournir celle-ci aux éditeurs intéressés à un prix orienté vers les coûts. La mise en place de cet organisme a été renvoyée par la loi à un décret en Conseil d'État qui n'est pas intervenu en raison des modifications du contexte juridique européen. Ce sont les dispositions de l'article 6 de la directive 98/10/CE qui sont à l'origine de ce changement d'orientation. Elles imposent à tout opérateur l'obligation de céder à un tarif orienté vers les coûts sa liste d'abonnés à toute personne qui en fait la demande en vue d'éditer un annuaire universel. Cette obligation prive l'organisme ; dont la création avait été envisagée par le législateur, de la perspective de jouir de la gestion exclusive de la liste universelle, et l'expose à une concurrence éventuelle qui pourrait compromettre son équilibre financier. C'est pourquoi le Gouvernement souhaite qu'une modification législative soit apportée afin, d'une part,

de transporter en droit français les dispositions de l'article 6 de la directive 98/10/CE et d'autre part, de supprimer la référence à l'organisme prévu à l'article L. 35-4 du code des postes et télécommunications. Tout éditeur aura la faculté de s'adresser à chacun des opérateurs afin d'obtenir communication de sa liste d'abonnés, en vue de publier un annuaire. France Télécom continuera, comme par le passé, d'être chargée d'éditer un annuaire universel et d'assurer un service de renseignement universel dans le cadre de ses obligations de service universel. Elle aura la possibilité, pour remplir effectivement cette obligation, de s'adresser à chacun des opérateurs pour obtenir les listes d'abonnés nécessaires. La mise en place effective de l'annuaire universel est liée à la modification législative envisagée dont le Gouvernement souhaite qu'elle intervienne à échéance rapprochée. Le secrétariat d'État à l'industrie prépare d'ores et déjà les textes d'application du dispositif législatif qui seraient nécessaires. Ceux-ci feront l'objet d'une large concertation avec les acteurs notamment sur les questions liées aux modalités techniques de la cession des listes d'abonnés, à la présentation des informations dans l'annuaire universel et à la protection des données à caractère personnel et de la vie privée.

Accès aux réseaux de radiotéléphonie mobile

24412 – 13 avril 2000 – M. Pierre André attire l'attention de M. le secrétaire d'État à l'industrie sur l'inégalité d'accès aux réseaux de radiotéléphonie mobile, à juste titre dénoncée par les élus et les habitants de communes rurales du département de l'Aisne qui se trouvent exclus d'un service qui constitue un enjeu, non seulement en matière d'aménagement du territoire, mais aussi en matière d'amélioration de la qualité de vie. Cette exclusion est d'autant plus vivement ressentie comme une injustice inadmissible par les habitants de ces zones non couvertes par un des réseaux de téléphonie mobile qu'elle leur est imposée à partir de critères de pure rentabilité. En effet, la couverture du territoire suit une logique strictement commerciale qui pénalise les habitants des territoires les moins peuplés et, souvent, les plus fragiles où le téléphone mobile serait encore plus qu'ailleurs utile aux particuliers pour joindre en cas d'urgence, notamment sur les routes, les services de santé ou de secours et aux communes rurales pour faciliter le développement ou le maintien de leurs activités économiques. Aussi il lui demande s'il entend mettre, le plus rapidement possible, un terme à cette forme de discrimination territoriale par une politique volontariste d'incitation financière en s'attachant à inclure la couverture du territoire par un réseau de radiotéléphonie dans la liste des services universels ou obligatoires, dans la perspective d'une véritable et réelle politique d'aménagement du territoire.

Réponse – 6 juillet 2000 – Le Gouvernement attache une grande importance au développement de la téléphonie mobile qui constitue un outil important au service de l'aménagement du territoire. S'agissant de la couverture nationale, les opérateurs GSM ont respecté et même dépassé les obligations de leur licence avec plusieurs années d'avance : plus de 95 % de la population française a désormais accès aux services de France Télécom, SFR ou Bouygues Télécom. Chaque opérateur, dans le cadre de sa stratégie commerciale,

poursuit ses programmes d'investissements destinés à étendre la couverture du territoire en mobiles et à améliorer la qualité du service dans les zones déjà couvertes. Cependant les dernières fractions du territoire sont les plus difficiles et les plus coûteuses à couvrir. Dans ce contexte, le Gouvernement souhaite favoriser toutes les solutions qui permettent de compléter la couverture du territoire par les réseaux de radiotéléphonie : une coopération plus importante entre les parties prenantes (grâce à des accords d'itinérance, à une mutualisation des infrastructures...) dans le respect du droit de la concurrence, de même que le développement de systèmes de communications mobiles par satellite devraient ainsi permettre d'offrir l'accès au réseau dans les zones non couvertes ou particulièrement isolées. Dans certaines régions, des discussions sont en cours entre les opérateurs GSM et les collectivités locales afin d'étudier les modalités qui permettraient d'étendre la couverture des opérateurs. Celles-ci peuvent donner lieu à une intervention financière des collectivités locales ou à un financement par les fonds structurels européens (FEDER) la Commission européenne ayant donné son accord pour qu'il permette l'amélioration de la couverture GSM dans un état membre de l'Union européenne. Le rapport du Gouvernement sur le service public des télécommunications qui sera adressé au Parlement avant la fin du premier semestre de l'année 2001 fournira l'occasion de faire un bilan complet des résultats obtenus et escomptés de ce domaine.

Téléphones portables – appels d'urgence – centres de traitement – fonctionnement

42220 – 28 février 2000 – M. Hervé Gaymard appelle l'attention de M. le secrétaire d'État à l'industrie sur les difficultés que rencontrent les centres de traitement de l'alerte (CTA) du fait des nombreux appels injustifiés en provenance du 112 (numéro d'appel unique européen), qui sont le fait d'utilisateurs de téléphones portables. L'une des difficultés que rencontrent les CTA est de trier ces appels injustifiés. Ceux-ci, dans les périodes de « pics d'intervention », peuvent représenter jusqu'à 50 % du volume de trafic téléphonique des CTA, créant ainsi des dysfonctionnements importants. En effet, tous les téléphones portables permettent d'appeler le 112, avec ou sans code d'accès, avec ou sans carte d'abonnement, avec ou sans possibilité d'identifier l'appelant, lorsque la carte SIM est retirée. Cependant, même lorsqu'aucune identification n'est possible, le numéro de série de l'appareil s'affiche, l'opérateur peut donc repérer un appel injustifié lorsqu'il est répété, ce qui est très souvent le cas. Il suffirait donc, lorsqu'un appel émanant d'un portable est jugé indispensable, que l'opérateur dispose d'un moyen de le basculer sur un répondeur, qui le renverrait, pendant vingt-quatre ou quarante-huit heures, sur le 18, le 17 ou le 15, qui ne peuvent être obtenus sans carte SIM. Un tel dispositif serait, sans doute, dissuasif pour les personnes qui s'adonnent à des pratiques peu responsables. Par exemple, il peut s'agir d'enfants qui utilisent « le portable » comme un jouet. Le record en la matière, relevé au CTA de Savoie, est de cent appels à l'heure par le même intervenant. Il demande si, sur la base de l'idée ci-dessus décrite, des aménagements techniques pourraient être envisagés, afin de mettre fin à une source

de dysfonctionnements non négligeables pour les services qui ont en charge les secours et la sécurité des personnes, et qui doivent agir avec la plus grande efficacité.

Réponse. – 7 août 2000 – L'autorisation, délivrée aux opérateurs de radiotéléphonie, d'exploiter un réseau de télécommunications ouvert au public en vertu des dispositions de l'article L 33-1 du code des postes et télécommunications leur fixe des obligations. C'est ainsi qu'ils doivent prendre « toutes » les mesures nécessaires pour acheminer gratuitement les appels à destination des services publics chargés de la sauvegarde des vies humaines, des interventions de police, de la lutte contre l'incendie, de l'urgence sociale, vers le centre compétent correspondant à la localisation de l'appelant... « . Cette disposition d'intérêt général s'inscrit dans le cadre de la sécurité publique. Les services de secours destinataires des appels ont, lors de la communication, connaissance du numéro de l'appelant, y compris pour les numéros classés en liste rouge et lorsque la fonction secret est activée. Cette mesure permet, pour les appels passés à partir du réseau fixe, de localiser l'origine de l'appel et d'envoyer les secours même lorsque l'interlocuteur est incapable d'indiquer sa position. Le même dispositif existe pour les appels passés à partir des mobiles alors que les réseaux ne permettent pas actuellement de localiser instantanément l'appelant. Il est ainsi possible aux services de secours de connaître l'identité de l'abonné dont le terminal est à l'origine de l'appel. Lorsque le terminal n'est pas équipé de carte SIM ou lorsque celle-ci a été désactivée par l'opérateur, l'appel du 112 est encore possible et les services d'urgence ont alors connaissance du numéro de série du terminal utilisé ce qui rend possible l'identification de la personne l'ayant acquis. La possibilité d'appel du 112 sans carte SIM ou lorsque celle-ci est désactivée répond elle aussi à un souci de sécurité publique qui vise à étendre au maximum la possibilité d'alerte des services de secours (pompiers et SAMU) lorsque des vies humaines sont en jeu. C'est pourquoi il ne saurait être questions de la supprimer. S'agissant des appels « parasites », plusieurs situations se présentent qui vont de l'erreur manifeste (112 composé en lieu et place du 12), à l'appel malveillant émanant de personnes ne sachant pas qu'elles peuvent être identifiées en passant par l'usage intempestif (notamment de jeunes enfants utilisant un terminal comme jouet). La configuration technique des réseaux des opérateurs ne permet pas de prendre une mesure telle que celle envisagée par l'honorable parlementaire dans la mesure où le routage des appels n'est pas effectué au niveau du terminal mais au point d'interconnexion avec le réseau fixe et concerne tous les appels ; chaque appel vers un numéro abrégé est routé vers le numéro transcrit correspondant au service d'urgence appelé compétent géographiquement. Il convient d'une part d'éviter que les comportements inciviques ne se multiplient et d'autre part de sanctionner ceux qui sont de nature à mettre en péril la vie de nos concitoyens en risquant de saturer le centre de traitement des appels. C'est pourquoi les appels malveillants et répétitifs doivent faire l'objet d'un signalement aux procureurs de la République qui leur donnent la suite qui s'impose.

Coût des télécommunications entre les DOM et la métropole

24809 – 4 mai 2000 – M. Rodolphe DESIRE attire l'attention de M. le secrétaire d'État à l'industrie sur le problème posé par la tarification élevée des communications téléphoniques entre les départements d'outre-mer et la France métropolitaine. En effet, si l'on dresse un bilan des tarifs pratiqués par France Télécom en dépit de la concurrence a priori effective dans ce secteur depuis 1998, on constate que la tarification est encore essentiellement basée sur la distance géographique qui sépare deux points d'un même territoire. D'autre part, l'argument technique généralement avancé des moyens spécifiques onéreux à mettre en œuvre pour l'exploitation de ces relations téléphoniques manque aujourd'hui de pertinence, dans la mesure où les satellites disponibles sont actuellement plus nombreux, les câbles transcontinentaux plus efficients et la possibilité d'utiliser la technologie internet devenue une réalité. Ainsi, à titre d'exemple, les principales entreprises américaines du secteur des télécommunications ont d'ores et déjà mis en place des tarifs à la minute applicables à tous les appels téléphoniques effectués sur le territoire des cinquante États, aussi bien à l'intérieur d'un État particulier qu'entre la Floride et Hawaï. En conséquence, il souhaite connaître son sentiment sur la nécessité de favoriser la notion de cohérence territoriale en demandant à l'opérateur national dont l'État détient encore à ce jour la majorité des parts de diminuer le prix des communications entre les régions ultra-périphériques et la France continentale. Sans aucun doute, une telle initiative unifiant les tarifications en cours renforcerait encore davantage le sentiment d'appartenance à l'Union européenne que manifestent les habitants des départements d'outre-mer. En outre, l'abaissement des coûts des télécommunications améliorerait sensiblement la position concurrentielle des entreprises locales en réduisant leurs factures vis-à-vis de la métropole. Il le remercie des précisions qu'il voudra bien apporter sur ce point aux particuliers et entrepreneurs antillais soucieux de voir amenuisés les effets néfastes de l'insularité et de l'éloignement géographique.

Réponse – 3 août 2000 – La téléphonie vocale à partir des postes fixes relève du service universel des télécommunications. L'article L. 35-2 de la loi de réglementation des télécommunications du 26 juillet 1996 précise que le cahier des charges de France Télécom détermine notamment « les obligations tarifaires nécessaires (...) pour éviter une discrimination fondée sur la localisation géographique ». La péréquation géographique des tarifs s'applique en ce qui concerne l'abonnement comme les communications. S'agissant cependant du prix des communications, la péréquation géographique des tarifs s'exerce dans le cadre de tranches de distance déterminées. Cette segmentation tarifaire par tranche de distance n'est nullement contraire au principe d'égalité associé à la prestation de service universel, qui est compatible avec la prise en compte de la situation particulière de certaines catégories d'usagers. En effet, malgré les progrès technologiques, dont il fait état, la distance reste une variable déterminante du prix des communications. En revanche, ces progrès technologiques, conjugués à l'augmentation tendancielle du trafic et au développement de la concurrence, ont permis une baisse significative du prix des télécommunications au départ et à destination des

départements d'outre-mer. En termes de tarifs, hors prise en compte du crédit-temps, la minute de communication en cinq ans est passée de 5,59 francs hors taxes à 1, 96 franc hors taxe. Cet abaissement du prix des communications, dans un contexte de concurrence croissante, ne peut que contribuer à l'amélioration de la position concurrentielle des entreprises locales. Le contexte concurrentiel est également favorable au développement d'innovations tarifaires, France Télécom ayant notamment mis en place récemment des forfaits de communications entre les DOM et la métropole.

Échelon

Réseau Échelon – attitude de la France

42879 – 6 mars 2000 – M. Jean-Luc Warsmann attire l'attention de M. le Premier ministre au sujet du réseau anglo-saxon Échelon d'espionnage des télécommunications au niveau mondial. Le débat au Parlement européen sur le réseau Échelon a suscité de nombreux échos en Europe et en France. De nouvelles preuves seraient apparues selon lesquelles une partie de la vocation de ces installations est commerciale alors que le Gouvernement américain fait traditionnellement valoir des impératifs de défense. Selon cette étude, le réseau Échelon permettrait d'intercepter dans le monde entier les communications transmises par voie satellitaire, qu'il s'agisse de messages téléphoniques, de fax ou de courrier électronique via internet. Aussi, il souhaiterait connaître la position du Gouvernement sur cette étude et les moyens qu'entend mettre en œuvre le Gouvernement pour assurer la sécurité des communications. Question transmise à M. le ministre de la défense.

Réponse – 15 mai 2000 – Le « réseau Échelon de surveillance et d'interception des télécommunications à l'échelle mondiale » a été mis en place, à l'origine, pour des raisons de sécurité militaire. Selon deux rapports remis au Parlement européen, il aurait été utilisé à des fins d'espionnage économique. Face à ce possible détournement d'objectif, le Parlement européen, dans une résolution de septembre 1998, a appelé à la mise en place de systèmes de contrôle public et à l'adoption de mesures de cryptage et de protection des informations économiques. Le recueil d'informations dans un objectif de sécurité nationale a toujours été nécessaire. Cependant, l'accroissement des échanges de données et des réseaux d'informations multiplie les risques d'interception, de piratage de données sensibles ou d'atteintes à la vie privée. De plus, l'interconnexion de ces réseaux ouverts avec les réseaux internes des entreprises renforce les possibilités d'accès parasites à des informations sensibles. Pour se prémunir de tels risques, chaque pays s'est doté d'une législation visant à protéger les atteintes à la vie privée. En ce qui concerne la France, l'article 226-1 du code pénal punit « d'un an d'emprisonnement et de 300 000 francs d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui, en captant enregistrant ou transmettant sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ». Par ail-

leurs, la loi du 10 juillet 1991 relative au secret des correspondances émises par les télécommunications garantit, en son article 1er, les particuliers contre les interceptions opérées hors du cadre de cette loi. Elle institue notamment une Commission nationale de contrôle des interceptions de sécurité, qui peut être saisie par toute personne y ayant un intérêt direct et personnel. Au-delà de ces barrières juridiques, il est indispensable que les administrations et les entreprises développent une culture de protection de l'information sensible, en particulier dans le cas d'un transfert par satellite de rediffusion. Dans ce cadre, le ministre de la défense a nommé un directeur de la sécurité des systèmes d'information qui assure la coordination des politiques de sécurité de tous les états-majors, services et directions de son ministère. D'autres initiatives concernant le secteur civil ont été prises par le Gouvernement. Ainsi, lors du comité interministériel du 19 janvier 1999, le Premier ministre a annoncé une modification de cadre législatif français en matière de cryptologie visant à offrir une liberté complète dans l'utilisation des moyens de chiffrement utilisant des clés allant jusqu'à 128 bits, ce qui constitue un niveau qui permet d'assurer une grande sécurité. De plus, le Gouvernement a décidé au début de cette année, de mettre en place un centre de veille, de prévention et de secours chargé de coordonner les efforts des administrations pour faire face aux attaques informatiques. C'est dans cette optique qu'une direction de la sécurité des systèmes d'information auprès du Premier ministre a été créée. Par ailleurs, des mesures complémentaires de protection des informations industrielles sont également à l'étude et seront soumises d'ici à quelques mois au Parlement.

Cryptologie

Réseaux de données – cryptologie – réglementation

28690 – 19 avril 1999 – M. Olivier de Chazeaux appelle l'attention de M. le secrétaire d'État à l'industrie sur les dispositions de l'arrêté du 17 mars 1999 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisations relatives aux moyens et prestations de cryptologie. Cet arrêté fait référence dans la partie technique à « un dossier préalablement déposé pour un produit usant du même procédé de cryptologie ». La question se pose de savoir par quel moyen le service central de sécurité des systèmes informatiques va informer l'industriel du contenu du « dossier préalablement déposé ». Il s'agit là en effet d'un enjeu industriel considérable dans la mesure où la référence à un dossier précisément défini permet de créer une liste de référentiels où les produits sont déjà recensés. Dès lors qu'un industriel se référera à tel ou tel produit préalablement défini, il s'exonérera d'une expertise juridique et technique coûteuse qui seule permet en réalité de satisfaire pleinement aux conditions de l'arrêté. C'est pourquoi il lui demande de bien vouloir définir la nature exacte de ce dossier et les droits que fera naître la référence à ce dernier. Question transmise à M. le Premier ministre.

Réponse – 29 mai 2000 – L'honorable parlementaire attire l'attention de M. le Premier ministre sur la question des modalités de description des produits et prestations de cryptologie soumis à déclaration ou autorisation. L'arrêté du 17 mars 1999 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptologie prévoit que ce dossier comprend une partie technique relative à la description du produit concerné. Cette description comporte notamment « soit la description complète des procédés de cryptologie employés, sous la forme d'une description mathématique et d'une simulation dans un langage de haut niveau, type C ou Pascal », « soit la référence à un dossier préalablement déposé pour un produit usant du même procédé de cryptologie, soit la référence à un standard reconnu, non équivoque, et dont les détails techniques sont accessibles aisément et sans condition ». Les deux alternatives à la description mathématique accompagnées d'une simulation ont été prévues afin de faciliter aux industriels la description demandée. La première (référence à un dossier préalablement déposé) figurait déjà dans l'arrêté du 13 mars 1998, la seconde (référence à un standard reconnu) est une innovation de l'arrêté du 17 mars 1999. La première alternative était admise ; en pratique depuis plusieurs années. Le SGDN (SCSSI) acceptait, dès avant sa consécration par les textes, qu'un industriel fasse référence à des dossiers qu'il avait lui-même préalablement déposés, voire à des dossiers déposés par un autre industriel dont il intégrait des modules ayant des fonctions cryptologiques. Cette deuxième hypothèse était néanmoins plus rare, et parfois déconseillé par le SGDN (SCSSI) : le dossier technique déposé par un industriel n'étant pas communiqué, les références que pouvaient en faire d'autres industriels risquaient d'être inappropriées, ce qui aboutissait à compliquer et donc à ralentir le traitement des dossiers ; la pratique était néanmoins admise en cas de réutilisation complète d'un produit ou d'un module bien précis, ayant fait l'objet d'un dossier technique, dans un autre produit soumis à autorisation ou déclaration. Cette possibilité mise en œuvre avec pragmatisme par le SGDN (SCSSI), ne semble par avoir suscité de problème jusqu'à présent. Mais il n'est pas envisagé, au-delà de cette commodité désormais consacrée par les textes, de mettre à disposition des industriels une liste de produits déclarés ou autorisés de leurs concurrents, assortie des informations techniques afférentes, qui pourrait servir de référentiel dans le cadre de la description d'un produit. Le SGDN (SCSSI) publie sur son site internet une liste de produits déclarés et autorisés, mais seulement après accord formel des industriels concernés, et sans information technique : systématiser cette publication et l'assortir d'informations techniques se heurterait en revanche aux obstacles suivants : en aucun cas le SCSSI ne publie le contenu d'un dossier déposé ; il est au contraire tenu de veiller à la confidentialité des informations qui lui sont communiquées (art. 26 du décret n° 98-101 du 24 février 1998 définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie) ; tout au plus, dans le cadre d'une relation directe avec un industriel, le SCSSI peut faire savoir à celui-ci s'il est nécessaire ou non de décrire un procédé de cryptologie non publié ; la déclaration par réfé-

rence peut-être source de confusion et d'erreurs dès lors que le dossier référencé, tel qu'il a été déposé par un industriel, n'est pas complètement connu des autres industriels ; en outre, su un produit s'avérait, après examen, non conforme à sa description, tous les dossiers faisant référence à celui déposé pour ce produit seraient entachés du même défaut, mais sans qu'il soit nécessairement possible d'obtenir les informations nécessaires auprès de l'industriel originel, au moment où la non-conformité serait mise en évidence. La deuxième alternative (référence à un standard reconnu), était également admise par le SGDN (SCSSI), en pratique, depuis plusieurs années. Sa consécration par les textes, entérinant cette pratique, n'a donc soulevé aucun problème pour les industriels et le SGDN (SCSSI). Le caractère de standard reconnu dont les détails techniques sont accessibles aisément et sans condition ne semble pas avoir posé de problème d'interprétation tant pour les procédés de cryptologie que pour les autres informations du dossier technique. En cas de doute portant sur l'implémentation d'un standard reconnu (la plupart des standards permettent plusieurs implémentations qui ont laissé au choix de l'industriel : pour les algorithmes de chiffrement par exemple, RC444, blowfish, AES, etc..., la longueur de la clé n'est généralement pas fixée a priori), les incertitudes sont rapidement levées grâce aux contacts directs entre le SGDN (SCSSI) et l'industriel concerné. Le SGDN (SCSSI) n'a donc pas jugé utile de publier des précisions sur cette disposition. Il n'a d'ailleurs pas reçu de demande dans ce sens de la part des industriels.

Réseaux de données – cryptologie – réglementation

29081 – 26 avril 1999 – M. Olivier de Chazeaux appelle l'attention de M. le secrétaire d'État à l'industrie sur les dispositions du décret n° 98-101 du 24 février 1998 définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie. L'article 6 de ce décret fait référence à un délai d'un mois laissé au service central de sécurité des systèmes informatiques pour se prononcer sur la nature du régime applicable au moyen ou à la prestation de cryptologie. La question se pose de savoir si, à l'expiration du délai d'un mois, le moyen ou la prestation concernés bénéficient alors d'une présomption irréfragable établissant qu'ils ne relèveront plus du régime d'autorisation. Il s'agit d'une question déterminante au regard des exigences de sécurité juridique afin d'éviter le risque de basculement d'un régime dans un autre. C'est pourquoi il lui demande d'apporter des éléments de réponse sur cette question. – Question transmise à M. le Premier ministre.

Réponse – 29 mai 2000 – L'honorable parlementaire attire l'attention de M. le Premier ministre sur la question des conditions de mise sur le marché d'un produit ayant fait l'objet d'une déclaration, une fois expiré le délai d'un mois laissé à l'administration pour se prononcer sur le régime applicable à ce produit. Le décret N° 91-101 du 24 février 1998 définissant les conditions dans lesquelles sont souscrites les déclarations accordées les autorisations concernant les moyens et prestations de cryptologie dispose, en son article 6, que « si le moyen ou la prestation de cryptologie déclaré relève du régime de

l'autorisation, le service central de la sécurité des systèmes d'information, dans le délai d'un mois à compter de la demande à laquelle le dossier a été reçu ou, le cas échéant, complété, invite, par lettre recommandée avec demande d'avis de réception, le déclarant à procéder à l'application des dispositions du titre III (relatives au régime d'autorisation). À l'expiration du délai d'un mois, et en cas de silence du service central de la sécurité des systèmes d'information, le déclarant peut procéder librement aux opérations faisant l'objet de la déclaration ». Il incombe au SGDN (SCSSI) de se prononcer, dans le délai imparti par les textes, sur le régime applicable au produit concerné. Les textes prévoient expressément qu'une fois ce délai expiré, le silence de l'administration permet de « procéder librement aux opérations faisant l'objet de la déclaration ». Ces opérateurs – dans la limite de ce qui figure dans la déclaration, et sous réserve naturellement que celle-ci ne soit entachée d'aucune irrégularité ou fraude – ne saurait donc, passé ce délai et à défaut d'observations du SGDN (SCSSI), être soumise à aucune formalité nouvelle.

Divers

Archives des services de renseignement

24667 – 27 avril 2000 – M. René Trégouët rappelle à l'attention de M. le ministre de la défense la publication récente de certaines archives de la CIA datant de 1953 et concernant l'Iran. Il lui demande à cette occasion de bien vouloir lui rappeler les règles appliquées en France concernant la publication des archives de ses services de renseignement.

Réponse – 29 juin 2000 – La loi n° 79-18 sur les archives définit clairement les délais au-delà desquels les documents d'archives publiques peuvent être librement consultés. Le délai de base est de trente ans, à l'exception des documents de nature particulière, notamment ceux mettant en cause la vie privée ou intéressant la sûreté de l'État ou la défense nationale, pour lesquels ce délai est porté à soixante ans. De plus l'article 6 du décret n° 79-1035 du 3 décembre 1979 relatif aux archives de la défense dispose que ne peuvent être communiqués qu'après un délai de soixante ans, « les dossiers, rapports et fiches de renseignements à caractère nominatif mettant en cause la vie privée ou intéressant la sûreté de l'État ou la défense nationale, les dossiers des deuxièmes bureaux des états-majors et des bureaux de renseignement et de relations internationales militaires, et les dossiers du service de documentation extérieure et de contre-espionnage ». Ainsi, sous réserve de ces conditions de délais, toute personne a le droit de consulter, dans des locaux réservés à cet effet par les différents services historiques, les archives communicables dans leur forme originale ou sous forme de copie, lorsque leur conservation matérielle ou les conditions de stockage l'imposent. En tout état de cause, un document d'archives peut être communiqué par dérogation aux règles générales soumise au ministre de la défense et après avis du service détenteur des archives. L'autorisation de consultation par dérogation

mentionne expressément la liste des documents qui peuvent être communiqués, l'identité des personnes admises à en prendre connaissance et le lieu où les documents peuvent être consultés. En outre, elle précise, le cas échéant si leur reproduction peut être effectuée et en détermine les modalités. Toutefois, la dérogation accordée revêt un caractère précaire et révocable. Elle est notamment limitée dans le temps et peut être retirée si les conditions dans lesquelles elle a été accordée ne sont plus respectées par le demandeur. Compte tenu du caractère sensible des informations contenues. Il est également possible d'ouvrir au public, par le biais de dérogations générales, l'accès à certains fonds ou parties de fonds, dès lors que les documents qui les composent ont une ancienneté d'au moins trente ans. Tel est le sens de l'arrêté du 28 décembre 1998, pris à la suite d'une directive du Premier ministre. Il concerne l'ouverture des fonds d'archives de la défense pour la période du 1er janvier 1939 au 31 décembre 1945, gérés par les services d'archives du ministère de la défense, à l'exception des dossiers, rapports et fiches de renseignements à caractère nominatif mettant en cause la vie privée des personnes citées.

Ecoutes téléphoniques

9804 – 23 juillet 1998 – M. Jean-Pierre Cantegrit appelle l'attention du M. le ministre de l'intérieur sur le problème des écoutes téléphoniques à propos desquelles il a pris acte de la déontologie affirmée à plusieurs reprises par le Gouvernement auquel il appartient et espère que celle-ci est strictement respectée. D'après des informations qui lui ont été communiquées, il apparaîtrait que l'un des centres parisiens de ces écoutes serait installé aux Invalides. Il lui indique que les porteurs de postes téléphoniques mobiles, qu'ils soient installés dans un véhicule ou qu'ils soient portables, voient leurs communications systématiquement interrompues lorsque ces dernières sont effectuées à proximité du périmètre du centre souterrain des Invalides. En conséquence, il lui demande si l'évolution des moyens techniques ne permettrait pas aux Français qui utilisent des téléphones mobiles de ne pas voir leurs communications interrompues en raison de l'installation d'un centre d'écoutes et d'interceptions dans ce périmètre, et donc de ne pas être taxés par là même d'une communication téléphonique supplémentaire. Il serait heureux qu'une réponse technique lui soit apportée sur cette question. – Question transmise à M. le Premier ministre.

Réponse – 27 avril 2000 – L'honorable parlementaire attire l'attention de M. le Premier ministre sur l'utilisation des téléphones mobiles à proximité du centre d'écoutes et d'interceptions téléphoniques des Invalides. Les installations techniques du groupement interministériel de contrôle ne peuvent en aucun cas perturber le réseau radioélectrique GSM. Les interceptions que cet organisme effectue sur les cibles utilisatrices sont réalisées, conformément à la réglementation, au niveau filaire à distance du centre d'exploitation et en aucun cas dans la partie hertzienne.

Organisme pour le contrôle des modalités d'exécution des écoutes téléphoniques judiciaires

15673 – 15 avril 1999 – M. Hubert Haenel demande à M^me^ le garde des sceaux, ministre de la justice, si elle envisage de créer un organisme indépendant, présidé par exemple par le premier président de la Cour de cassation, chargé de contrôler les modalités d'exécution des écoutes téléphoniques ordonnées par les magistrats de l'ordre judiciaire.

Réponse – 24 février 2000 – La ministre de la justice porte à la connaissance de l'honorable parlementaire que la création d'un organisme spécialement chargé de contrôler les modalités d'exécution des écoutes téléphoniques ordonnées par les juges d'instruction ne paraît pas d'actualité dans la mesure où les dispositions du code de procédure pénale assurent, d'ores et déjà, un contrôle légal et juridictionnel suffisant. En effet, si l'article 100 alinéa 2 du code de procédure pénale dispose que la décision d'interception des communications téléphoniques n'a pas de caractère juridictionnel et est insusceptible de recours, il convient de considérer les éléments suivants : en premier lieu, les conditions de fond et de forme des écoutes téléphoniques judiciaires sont strictement définies aux articles 100 à 100-7 du même code. De telles investigations sont réservées à la recherche d'infractions d'une certaine gravité, pour une durée limitée, si les nécessités de l'instruction l'exigent. De plus, les opérations techniques d'interception et d'enregistrement sont exécutées par des agents qualifiés, la correspondance utile à la manifestation de la vérité est transmise par le magistrat instructeur ou un officier de police judiciaire commis par lui, les enregistrements sont placés sous scellés fermés et détruits à l'expiration du délai de prescription de l'action publique. Enfin, aucune interception de communication téléphonique ne peut avoir lieu sur la ligne d'un député, d'un sénateur ou d'un avocat sans que le président de l'Assemblée nationale, le président du Sénat ou le bâtonnier respectivement en soit avisé par le juge d'instruction ; en second lieu, les procès-verbaux de transcription, versés au dossier d'information, sont des pièces soumises à l'appréciation et à la discussion des parties comme toute pièce de procédure résultant d'un acte d'investigation ordonné par le magistrat instructeur et sont à ce titre soumis à la règle commune du contrôle par la chambres d'accusation, juridiction collégiale d'instruction du second degré.

Téléphones portables dans les établissements pénitentiaires

18802 – 16 septembre 1999 – M. Emmanuel Hamel attire l'attention de M^me^ le garde des sceaux, ministre de la justice, sur l'information parue à la page 8 B du quotidien *Le Figaro* du 27 juillet 1999 selon laquelle lors de la fouille générale, organisée à la prison des Beaumettes « après l'évasion de cinq détenus par hélicoptère, le 28 juin dernier, huit appareils (téléphones portables) et un chargeur ont été retrouvés dans les égouts ». Il lui demande les mesures concrètes que les pouvoirs publics entendent mettre en œuvre pour améliorer la sécurité dans les prisons.

Réponse – 20 juillet 2000 – Le garde des sceaux, ministre de la justice, porte à la connaissance de l'honorable parlementaire que les pouvoirs publics sont soucieux du problème posé par l'introduction de téléphones portables dans les établissements pénitentiaires compte tenu notamment de la possibilité qu'offrent ces appareils pour communiquer avec des complices dans le cadre d'un projet d'évasion. Les chefs d'établissement sont sensibilisés à ce problème et appellent régulièrement les personnels pénitentiaires à la vigilance. La découverte de téléphones portables n'est toutefois pas aisée, en raison de la très faible quantité de leurs composants métalliques et de leur miniaturisation. Cependant, l'attention des personnels a permis à plusieurs de découvrir des téléphones portables lors de fouilles ou contrôles, aussi bien dans les locaux de détention que dans les zones extérieures aux bâtiments, tels que cours de promenade et terrains de sports. À cet égard, il convient de signaler que, lors de chaque découverte de téléphone portable lors d'une fouille, les détenus ont fait l'objet de procédures disciplinaires. À cinq reprises, des détenus ont été poursuivis pénalement. La solution qui consisterait à générer un système de brouillage empêchant l'utilisation des téléphones portables dans une enceinte pénitentiaire ne peut être envisagée. En effet, il n'existe en l'état actuel, aucun système de brouillage qui ne perturbe pas les systèmes électroniques existants. Au plan réglementaire, comme l'a rappelé dans un avis du 10 juin 1999 l'autorité de régulation des télécommunications, la mise en œuvre de ces systèmes est interdite en France, et les contrevenants sont passibles des peines prévues par l'article L39-1 du code des postes et télécommunications. Dans ce même avis, cette autorité exposait pourquoi elle n'était pas favorable à leur développement, de nature à remettre en question, d'une part, le respect, par les opérations mobiles, des obligations contenues dans leur autorisation ; obligation de fournir un niveau de qualité satisfaisant, obligation de couvrir une certaine proportion de la population, obligation d'acheminer les appels d'urgence ; d'autre part, dans le cas des systèmes « brouilleurs », le régime en vigueur d'attribution des fréquences utilisées entre les terminaux mobiles et les émetteurs radio. Les pouvoirs publics suivent avec attention les évolutions techniques en matière de sécurité, mais la mise en place de nouveaux systèmes de détection n'est envisageable que sous la double condition d'efficacité et de respect des règles en vigueur.

Délinquance et guerre informatiques

20982 – 2 décembre 1999 – M. Michel Moreigne attire l'attention de M. le Premier ministre sur la délinquance et la guerre informatiques. La lutte contre les intrusions illégales dans les systèmes d'information ou de télécommunication et contre les multiples formes du « cybercrime » devient une préoccupation majeure des entreprises de haute technologie, des services financiers, des services publics, des universités, etc. Ainsi, il lui demande quels sont les moyens humains et les infrastructures destinés à combattre l'augmentation des crimes électroniques, des délits et des risques de terrorisme informatiques, et à assurer la protection tans des entreprises, des structures vitales de notre pays que des citoyens. En outre, il lui demande

si, dans le cadre de la construction de l'Europe de la défense, ce domaine fera l'objet de coopération renforcée en dehors de l'OTAN (Organisation du traité de l'Atlantique Nord).

Réponse – 27 avril 2000 – L'honorable parlementaire attire l'attention de M. le Premier ministre sur les dangers du développement de la délinquance et de la guerre informatique. Face à la cybercriminalité, les mesures destinées à garantir la sécurité des systèmes d'information sont au cœur des préoccupations du Gouvernement. Le programme d'action gouvernemental pour la société de l'information (PAGSI) a pris en compte le besoin d'assurer la sécurité des réseaux et celui d'instaurer la confiance des usagers dans les nouvelles technologies de l'information et de la communication. Ainsi le comité interministériel pour la société de l'information du 19 janvier 1999 a-t-il décidé concrètement : d'une part des mesures de libéralisation de l'usage des procédés cryptologiques, ceux-ci constituant une réponse efficace à un certain nombre de vulnérabilités intrinsèques aux systèmes informatiques et de télécommunications ; d'autre part, la création d'un organisme d'alerte et de secours sur l'internet, dénommé CERT/A, destiné à assister les organismes de l'administration victimes d'agressions informatiques. Cette cellule est rattachée au service central de la sécurité des systèmes d'information (SCSSI) placé sous l'autorité du secrétariat général de la défense nationale (SGDN) ; enfin, un renforcement significatif des moyens de ce service central. Les premières mesures visant l'usage de la cryptologie sont entrées en vigueur dès la publication des décrets n^{os} 99-1999 et 99-200 du 17 mars 1999. Le premier décret libère, en particulier, l'utilisateur désirant recourir à un procédé cryptologique fort (utilisant une clef jusqu'à 128 bits) de toute formalité, dès lors que le produit a été déclaré par son fournisseur ou qu'il soit à l'usage privé d'une personne physique. Un projet de loi libéralisant complètement l'usage de la cryptologie est en chantier et sera soumis prochainement au Parlement. Le CERT/A, créé à la fin de l'année 1999, a été en mesure de participer à la veille instaurée pour assurer le paysage à l'an 2000 pour la partie malveillance informatique. Le SGDN a vu ses moyens augmenter de près de 20 % dès cette année, cette augmentation étant consacrée pour la plus grande partie à la protection des transmissions et réseaux gouvernementaux et à la sécurité des systèmes d'information. Le SCSSI sera transformé en direction centrale, avec des effectifs accrus en ingénieurs et techniciens, de façon à mettre les services français à un niveau comparable à ceux de ses principaux partenaires étrangers. Un directeur chargé de la sécurité des systèmes d'information au SGDN a été nommé en conseil des ministres sur proposition du Premier ministre le 15 mars 2000. Il reviendra au nouveau directeur de transformer le SCSSI en direction de plein exercice. Le SGDN s'est vu également confier la responsabilité de coordonner les réflexions interministérielles pour évaluer les vulnérabilités et les menaces pesant sur les infrastructures vitales du pays et de proposer les mesures à prendre pour y faire face. Ses conclusions seront adressées au Premier ministre durant l'été prochain. Par ailleurs, comme l'honorable parlementaire le sait, le Premier ministre, lors de son discours à Hourtin l'été dernier, a annoncé la création au ministère de l'intérieur, au sein de la direction générale de la police nationale, d'un office central de lutte contre la

criminalité liée aux technologies de l'information. Cet office centralisera les investigations concernant les crimes et délits traditionnels commis en ayant recours aux nouvelles technologies, ainsi que les crimes et délits ayant pour cibles ces technologies. La promulgation du décret de création de cet office est imminente. Naturellement, il serait vain pour un pays d'agir seul dans le contexte du cyberespace et c'est pourquoi le Gouvernement favorise la concentration et les initiatives internationales visant à promouvoir la confiance dans les nouvelles technologies et la sécurité sur les nouveaux réseaux. La France participe donc activement aux travaux du G 8 en matière de lutte contre la criminalité de haute technologie. C'est dans ce cadre que se tiendra à Paris, au moi de mai 2000, une conférence internationale réunissant plus de 300 personnes des administrations et du secteur industriel des huit pays, pour examiner les mesures susceptibles d'être prises pour garantir la sécurité dans ce nouvel espace, tout en veillant à préserver les libertés individuelles. En outre, la France a contribué avec ses principaux partenaires européens et nord-américains à l'élaboration de standards techniques de sécurité, aujourd'hui reconnus comme une norme mondiale. Ces critères communs doivent permettre de mesurer, de manière objective, des performances des produits proposés par le marché en matière de sécurité des technologies de l'information. Des accords de reconnaissance mutuelle des certificats établis selon cette norme ont déjà été signés par de nombreux pays, en France par le SGDN/SCSSI. Le projet de loi sur la signature électronique, adopté le 29 février 2000 par le Parlement, en conformité avec la directive européenne, constitue également un élément important pour la sécurisation du commerce électronique, puisqu'il contribue à garantir l'authenticité et l'intégrité des actes et transactions effectués de manière électronique. Enfin, la France a obtenu récemment que la sécurité soit prise en compte comme objectif prioritaire dans le plan d'action de la Commission européenne pour une Européenne électronique (cf document E-Europe du président de la commission, M. Romano Prodi). Ce domaine de la sécurité fera l'objet de la part du Gouvernement d'une attention particulière dans la construction de l'Europe de la défense. Ainsi, le Gouvernement, conscient des risques liés à l'usage des nouvelles technologies de l'information, est-il décidé à amplifier encore le volet de sécurité de sa politique en matière de société de l'information. Chacun attend de ces nouvelles technologies d'immenses retombées en terme de développement économique, social et culturel. Chacun doit, simultanément, s'attacher à parer aux vulnérabilités et risques nouveaux qu'elles peuvent entraîner. Le défi à relever concerne tous les acteurs, publics et privés, civils et militaires, les collectivités comme les simples citoyens. Il passe par des actions de sensibilisation et de formation, des actions de promotion des solutions de sécurité et des mesures de prévention et de répression, à la fois technique et juridique, des actes de malveillance de toutes natures. Ces actions sont largement engagées à l'initiative du Gouvernement. Elles seront poursuivies pour que les bénéfices escomptés de l'avènement des nouvelles technologies de l'information et de la communication soient effectivement au rendez-vous.

Jurisprudence française

Cour de cassation – Chambre criminelle

Arrêt du 12 janvier 2000.
Constat sur communications téléphoniques

REJET du pourvoi formé par la société E, et X, contre l'arrêt de la cour d'appel de Paris, 10e chambre, en date du 24 septembre 1998. (...)

(...) Sur le deuxième moyen de cassation, pris de la violation des articles 222-5, 225-7, 122-2 du code pénal, des articles 385, 512 , 515 et 593 du code de procédure pénale, violation de la Convention européenne des droits de l'Homme et des droits de la défense :

« en ce que l'arrêt attaqué a condamné X et la société E du chef de proxénétisme aggravé à des amendes pénales et à des dommages et intérêts ;

« aux motifs que la nullité des interceptions de communications privées opérées par les enquêteurs n'a pas été invoquée devant les premiers juges et ne saurait être examinée pour la première fois en cause d'appel ; que les constations opérées par les services de police ont permis de vérifier l'existence de messages prostitutionnels et l'absence de déconnexion de ces messages par les services télématiques ;

« alors, d'une part, que le moyen tiré de ce qu'une infraction de proxénétisme par le biais de la mise à disposition du public d'un service télématique n'a été constaté par les officiers de police judiciaire qu'en dissimulant leur qualité et en posant à leurs correspondants, qui n'affichaient aucun message prostitutionnel, des questions relatives à un tarif, n'est pas un moyen de nullité de la procédure mais un moyen de fond tiré de ce que l'infraction supposée n'a été que le fruit d'une provocation et d'un stratagème, et a été

provoquée par les autorités judiciaires et qu'elles ne pouvaient donc, de ce fait, faire l'objet d'aucune poursuite légale ; que la cour d'appel devait donc examiner le moyen, nonobstant le fait qu'il n'ait été invoqué qu'en cause d'appel ;

(...) Attendu qu'il ressort de l'arrêt et du jugement confirmé que les investigations de l'enquête ont consisté, pour l'essentiel, dans l'audition de personnes se livrant à la prostitution et recherchant leur clientèle par l'intermédiaire du serveur minitel exploité par la société E ainsi que dans les constatations faites par les policiers eux-mêmes sur le réseau télématique ;

Attendu que, pour déclarer irrecevable l'exception proposée par X, qui demandait l'annulation d'interceptions de communications émises par la voie télématique, opérées par la police en méconnaissance, selon le prévenu, des articles 100 et suivants du code de procédure pénale, l'arrêt attaqué constate que cette exception n'avait pas été présentée devant le tribunal correctionnel ;

Qu'en cet état la cour d'appel a fait l'exacte application de l'article 385, dernier alinéa, du code de procédure pénale ;

Qu'ainsi le moyen ne peut être accueilli ;

Sur le troisième moyen de cassation, pris de la violation des articles 225-5, 225-6, 225-7, 225-12 du code pénal, 226-15 du même code, 593 du code de procédure, défaut de motifs, manque de base légale :

« en ce que l'arrêt a déclaré X et la société E coupables de proxénétisme aggravé, et les a condamnés à des amendes pénales et à des dommages-intérêts ;

« aux motifs que la prostitution se développait par l'intermédiaire du service 3615 Aline, service de communication audiovisuelle exploité par les prévenus ; que les connexions effectuées par les services de police l'avaient été selon le procédé normal, accessible à tout public, et s'interrompaient seulement lorsque les interlocuteurs essayaient de transformer la communication audiovisuelle en un échange personnalisé sur une ligne téléphonique privée ; que les messages à caractère prostitutionnel n'étaient pas déconnectés, que X a favorisé en connaissance de cause un abondant réseau prostitutionnel dont il tirait, ainsi que société E, de considérables bénéfices ;

(...) « alors, qu'il résulte tant des éléments de l'enquête que des constatations des juges du fond que la partie des messages laissés sur le serveur télématique, accessible à un public indifférencié, n'est constitué que par les pseudonymes et cartes de visites permettant de connaître les personnes qui se sont inscrites dans le fichier du service ; qu'en revanche, dès lors que deux personnes inscrites dans ces fichiers décident de se connecter entre elles, toujours par l'intermédiaire du service télématique, leur conversation devient un échange privé, dont rien ne permet de dire qu'il serait accessible aux autres personnes se branchant sur le réseau, et qui est couvert par le secret de la correspondance et l'intimité de la vie privée ; qu'il résulte également du dossier que c'est uniquement à ce stade de connexion qu'ont eu lieu les

échanges « prostitutionnels » relatés par les policiers, le caractère prostitutionnel des pseudonymes et des cartes de visite n'étant ni établi ni constaté par les juges du fond ; que l'exploitant du service, s'il a la possibilité, dont il a usé en l'espèce, de déconnecter les personnes prétendant rentrer dans le service à l'aide d'éléments d'identification de nature prostitutionnelle, n'a en revanche aucun droit de s'immiscer dans les conversations fussent-elles engagées sur le serveur lui-même, ou fussent-elles de nature prostitutionnelle, nouées entre deux personnes s'étant légalement introduites dans le fichier du serveur ; qu'en déclarant les exploitants de ce service coupables de proxénétisme à raison du contenu, non des messages d'identification accessibles à tous, et relevant de leur contrôle, mais à raison de conversations privées engagées par deux personnes déterminées ayant décidé d'engager un contact réciproque sur le serveur, conversations sur lesquelles les exploitants de ce service n'avaient aucun droit de contrôle, sauf à violer le secret de la correspondance et de la vie privée, la cour d'appel a violé les textes susvisés ;

« alors, de surcroît, que ne saurait être considéré comme tirant profit de la prostitution d'autrui, le dirigeant d'un serveur télématique qui n'a pas le pouvoir de contrôler les conversations privées qui caractérisent seules des offres de prostitution et dont il ne peut connaître ni contrôler l'existence ;

« alors, enfin, que la cour d'appel ne caractérise à l'encontre des prévenus aucune des infractions assimilées au proxénétisme par l'article 225-6 du Code pénal ; que, notamment, il n'est constaté ni allégué qu'ils auraient servi d'intermédiaire entre une prostituée et un proxénète » ;

Attendu que les énonciations de l'arrêt attaqué mettent la Cour de cassation en mesure de s'assurer que la cour d'appel a, sans insuffisance ni contradiction, répondu aux chefs péremptoires des conclusions dont elle était saisie et caractérisé en tous ses éléments, tant matériels qu'intentionnel, le délit dont elle a déclaré les prévenus coupables, et a ainsi justifié l'allocation, au profit de la partie civile, de l'indemnité propre à réparer le préjudice en découlant ;

D'où il suit que le moyen, qui se borne à remettre en question l'appréciation souveraine par les juges du fond, des faits et circonstances de la cause ainsi que des éléments de preuve contradictoirement débattus, ne saurait être admis ;

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

REJETTE le pourvoi.

Cour de cassation – Chambre criminelle

Arrêt du 15 février 2000.
Sonorisation d'un local

(...) Sur le premier moyen de cassation, pris de la violation des articles 81, 100 et suivants, 57, 66, 152 du code de procédure pénale, 593 du même Code, 226-15 et 432-9 du code pénal, 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, défaut de motifs, manque de base légale, violation des droits de la défense ;

Attendu qu'il résulte de l'arrêt et des pièces de la procédure qu'à la suite de la découverte du corps d'R., atteint de deux balles de fort calibre, le juge d'instruction de Montpellier a délivré à la gendarmerie, le 12 décembre 1997, une première commission rogatoire pour déterminer les circonstances du meurtre, puis, le 25 décembre 1997, une nouvelle commission rogatoire en vue de « sonoriser, à l'occasion de la perquisition qui y sera effectuée, le domicile de M. », domicile que l'auteur présumé, était susceptible de fréquenter ;

Que, le lendemain, les officiers de police judiciaire ont procédé à une perquisition dans l'appartement de M. ; avec l'assistance de gendarmes du groupe d'observation et de reconnaissance de Versailles, qui y ont mis en place un équipement permettant de capter et d'enregistrer à distance les conversations ; qu'une nouvelle perquisition effectuée le 28 décembre a permis l'interpellation de Christophe V ; lequel a été mis en examen pour homicide volontaire le 30 décembre 1997 ;

Attendu que, pour rejeter la requête en annulation de la commission rogatoire du 25 décembre 1997, des opérations de sonorisation et de toute la procédure subséquente, déposée par l'avocat de V. après la notification de l'avis de fin d'information, l'arrêt énonce que « le magistrat instructeur était en droit, au visa tant de l'article 81 que des articles 100 et suivants du code de procédure pénale, d'autoriser, par une commission rogatoire technique, l'opération de sonorisation d'un appartement » et que les officiers de police judiciaire, qui ont agi dans un cadre légal défini par le juge d'instruction, « n'ont provoqué ni la venue de Christophe V. dans les lieux, ni les conversations qu'il y a librement entretenues avec M. »

Attendu qu'en cet état, le demandeur ne saurait se faire un grief de ce que la perquisition du 26 décembre 1997, qui ne pouvait avoir d'autres fins que la recherche d'objets utiles à la manifestation de la vérité, était irrégulière, dès lors que seul celui qui est personnellement victime a qualité pour invoquer une violation des règles de procédure, portant atteinte à l'intimité de la vie privée ;

D'où il suit que le moyen n'est pas recevable.

Cour de cassation – Chambre criminelle

Arrêt du 23 février 2000.
Atteinte à la vie privée, écoutes téléphoniques

(...) Statuant sur le pourvoi formé par B contre l'arrêt de la cour d'appel d'AIX EN PROVENCE 7e chambre, en date du 26 avril 1999, qui pour atteinte à la vie privée, l'a condamné à 10 mois d'emprisonnement avec sursis et 30 000 francs d'amende, et qui a prononcé sur les intérêts civils :

Vu le mémoire produit ;

Sur le moyen unique de cassation, pris de la violation des articles 226-1 du code pénal et 593 du code de procédure pénale, défaut de motifs, manque de base légale ;

« en ce que l'arrêt attaqué a déclaré B coupable d'atteinte à l'intimité de la vie privée par captation ou transmission des paroles d'une personne ;

« aux motifs que R a déclaré que B avait eu en charge les écoutes mises en place au domicile des époux WX, que Mme G a confirmé au cours de l'enquête que B avait participé à cette surveillance, que C a de même déclaré que B avait pris part à l'enquête, qu'en outre B, qui a admis avoir perçu des chèques de la société S, n'a pas été en mesure d'apporter des précisions sur l'origine de ces fonds ;

« alors que le délit prévu par l'article 226-1-1 du code pénal suppose, que être constitué, non seulement la captation, l'enregistrement ou la transmission des paroles prononcées par une personne dans un lieu privé, mais encore que les propos concernent l'intimité de la vie privée de cette dernière ; qu'en se bornant à relever, pour déclarer B coupable de ce délit, qu'il aurait eu en charge les écoutes téléphoniques mises en place au domicile des époux X et participé à leur surveillance aux dires des trois co-prévenus et qu'il n'avait pas justifié l'origine des fonds qu'il avait perçus de la société S, sans constater qu'il aurait lui-même capté, enregistré ou transmis des conversations des époux C, d'une part, ni relever que les paroles prononcées par ces derniers se rapportaient à l'intimité de leur vie privée, d'autre part, la cour d'appel n'a pas donné une base légale à sa décision » ;

Attendu que les énonciations de l'arrêt attaqué mettent la Cour de cassation en mesure de s'assurer que la cour d'appel a, sans insuffisance ni contradiction, répondu aux chefs péremptoires des conclusions dont elle était saisie et caractérisé en tous ses éléments, tant matériels qu'intentionnel, le délit dont elle a déclaré le prévenu coupable, et a ainsi justifié l'allocation, au profit de la partie civile, de l'indemnité propre à réparer le préjudice en découlant ;

D'où il suit que le moyen, qui se borne à remettre en question l'appréciation souveraine, par les juges du fond, des faits et circonstances de la cause, ainsi que des éléments de preuve contradictoirement débattus, ne saurait être admis ;

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

REJETTE le pourvoi.

Cour de Cassation – Chambre criminelle

Arrêt du 27 avril 2000.
Secret des correspondances, minitel

(...) Sur le premier moyen de cassation, pris de la violation des articles 226-15 et suivants du Code pénal, 591 et 593 du Code de procédure pénale, défaut de motifs, défaut de réponse à conclusions, manque de base légale ;

« en ce que l'arrêt attaqué a confirmé l'ordonnance de non-lieu du chef d'atteinte au secret des correspondances et reproduction ;

« aux motifs qu'il résulte de l'audition des agents ayant procédé aux constats relatifs au serveur 3615 X que ceux-ci se placent dans une position d'utilisateur, emploient des « pseudos » et des mots de passe, et utilisant un « logiciel de capture » , éditent le contenu des écrans ; qu'il résulte du constat relatif aux services Audiotel, qu'il suffit de faire le numéro proposé au public et de suivre les indications données verbalement ; qu'en procédant à la transcription de communications téléphoniques et à l'édition des informations contenues dans un écran de minitel, communications et informations ouvertes au public par la partie civile, moyennant paiement, et accessible à n'importe quel client de ce service, les agents de France Télécom n'ont commis aucun des délits visés à la plainte ; qu'en conséquence, leurs supérieurs n'ont pas commis les délits de recel et complicité ;

« alors, d'une part, que la chambre d'accusation n'a pas répondu au chef péremptoire du mémoire de la demanderesse faisant valoir que l'enregistrement et la transcription des communications téléphoniques avaient eu lieu sur provocation des agents de France Télécom comme le reconnaissait le témoin Y ce qui constituait la preuve que la reproduction de ces conversations était irrégulière ;

« alors, d'autre part, que, même si les conditions du délit prévu par l'article 432-9 du code pénal n'étaient pas remplies, le délit d'atteinte au secret des correspondances était constitué indépendamment de l'accès régulier du public au service télématique concerné, dès lors que les communications téléphoniques et que les informations contenues sur l'écran Minitel avaient été transcrites et éditées sans l'accord du fournisseur des services télématiques ; que, dès lors que l'élément matériel de l'atteinte au secret des correspondances par le biais de la reproduction était caractérisé, la cour d'appel, qui n'a pas tiré les conséquences de ses constatations, n'a pas légalement justifié sa décision en statuant comme elle l'a fait » ;

Sur le second moyen de cassation, pris de la violation des articles 432-1 et 432-2 du code pénal, 593 du code de procédure pénale, défaut de réponse à conclusions, défaut de motifs, manque de base légale ;

« en ce que l'arrêt attaqué a décidé n'y avoir lieu à suivre du chef des délits visés sans la plainte avec constitution de partie civile ;

« aux motifs qu'en procédant à la transcription de communications téléphoniques et à l'édition des informations contenues dans un écran de Minitel,

communications et informations ouvertes au public par la partie civile, moyennant paiement, et accessible à n'importe quel client de ce service, les agents de France Télécom n'ont commis aucun des délits visés à la plainte ;

« alors qu'en se prononçant ainsi, la chambre d'accusation n'a pas répondu au chef péremptoire du mémoire de la demanderesse qui soutenait que le délit de l'article 432-1 du code pénal, susceptible de correspondre aux faits objet de la saisine, était caractérisé en l'état de mesures prises par une personne dépositaire de l'autorité publique pour faire échec à l'exécution de la loi au mépris des stipulations contractuelles » ;

Les moyens étant réunis ;

Attendu que les énonciations de l'arrêt attaqué mettent la Cour de cassation en mesure de s'assurer que, pour confirmer l'ordonnance de non-lieu entreprise, la chambre d'accusation, après avoir analysé l'ensemble des faits dénoncés dans la plainte et répondu aux articulations essentielles du mémoire produit par la partie civile appelante, a exposé les motifs pour lesquels elle a estimé qu'il n'existait pas de charges suffisantes contre quiconque d'avoir commis les délits reprochés ;

Que la demanderesse se borne à critiquer ces motifs, sans justifier d'aucun des griefs que l'article 575 du Code de procédure pénale autorise la partie civile à formuler à l'appui de son pourvoi contre un arrêt de chambre d'accusation, en l'absence de recours du ministère public ;

Que, dès lors, en application du texte précité, qui, contrairement à ce que soutient la demanderesse, n'est pas incompatible avec les dispositions de l'article 61 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, la victime disposant d'un recours devant les juridictions civiles pour faire valoir ses droits, les moyens sont irrecevables et qu'il en est de même du pourvoi ;

Pour ces motifs,

DÉCLARE le pourvoi IRRECEVABLE ;

Cour de Cassation – Chambre criminelle

Audience publique du 14 juin 2000. Écoutes téléphoniques de lignes étrangères

REJET des pouvoirs formés par T, U, V, W, X, Y, Z contre l'arrêt de la chambre d'accusation de la cour d'appel d'Aix-en-Provence, en date du 3 février 2000, qui, dans l'information suivie contre eux du chef d'infractions à la législation sur les stupéfiants, a rejeté leurs requêtes en annulation d'actes de la procédure.

Sur le huitième moyen de cassation proposé par la société civile professionnelle Waquet, Farge et Hazan pour X, pris de la violation des articles 80, 81, 100 à 107, 151, 152, 170, 802 du code de procédure pénale, 1er de la Convention de l'entraide judiciaire en matière pénale, du principe de la territorialité des autorités étatiques :

« en ce que l'arrêt a refusé d'annuler les enregistrements téléphoniques retranscrits après écoute des lignes téléphoniques étrangères ;

« aux motifs que l'officier de police judiciaire qui, en exécution d'une commission rogatoire ne visant pas l'extension de compétence territoriale, pour procéder à l'interception, à l'enregistrement et à la transcription de communications émises sur une ligne téléphonique attribuée a un abonné qui demeure hors de son ressort territorial, ne méconnaît pas les règles de la compétence territoriale dès lors que tous les actes d'exécution de la commission rogatoire ont été dressés au siège de son service, dans lequel une déviation permettant l'écoute des conversations a été installée ; tel a bien été le cas en l'espèce et les écoutes ont été réalisées dans le strict respect des articles 100 à 100-7 du code de procédure pénale ;

« alors que le juge d'instruction ne peut, sans excéder ses pouvoirs, procéder à des actes d'instruction sur le territoire d'un État étranger ; que dès lors, l'écoute des lignes téléphoniques étrangères étant soumise à la législation nationale de chacun de ces pays, le juge d'instruction, et les officiers de police judiciaire par lui délégués, ne peuvent procéder eux-mêmes et directement, fût-ce au moyen d'une dérivation au siège de leur service, à l'écoute des lignes téléphoniques étrangères, sans avoir délivré une commission rogatoire à l'État étranger où doivent être effectuées ces écoutes téléphoniques » ;

Attendu que, pour rejeter le moyen de nullité présenté par X alléguant que le dossier contenait des transcriptions de conversations téléphoniques tenues dans des pays étrangers et enregistrées « peut-être par satellite » sur des lignes étrangères, en violation de l'intégrité territoriale de ces États, l'arrêt attaqué se prononce par les motifs reproduits au moyen ;

Attendu qu'en cet état, et dès lors qu'il ressort de l'examen des pièces de la procédure soumises au contrôle de la Cour de cassation et notamment des réquisitions délivrées en exécution des commissions rogatoires du juge d'instruction que les interceptions critiquées ont été réalisées dans les formes prévues par les articles 100 et suivants du code de procédure pénale et ont porté sur des correspondances émises depuis le territoire français, l'arrêt attaqué n'encourt pas les griefs allégués ;

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

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

Cour de cassation – Chambre criminelle

Arrêt du 25 octobre 2000.
Écoutes téléphoniques, messagerie télématique

(...) Sur le premier moyen de cassation, pris de la violation des articles 8 de la convention européenne des droits de l'Homme, 226-15, alinéa 2, du code pénal, 2 de la loi nº 86-1067 du 30 septembre 1986, 100 à 100-7 et 593 du code de procédure pénale, défaut de motifs, manque de base légale :

« en ce que l'arrêt attaqué a rejeté l'exception de nullité présentée par la société X, et est entré en voie de condamnation du chef de proxénétisme et l'a condamnée à une peine d'amende ;

« au motifs que le service télématique 3615 M est un service de communication audiovisuelle soumis à déclaration préalable en application de l'article 43 de la loi du 30 septembre 1986 et a pour objet de diffuser au public en général ou des catégories de public, en tout cas à des personnes susceptibles d'en prendre connaissance dans la seule limite où elles se connectent à un réseau accessible à tous ; que les annonces ainsi diffusées ne peuvent posséder le caractère de correspondance privée conformément à l'alinéa 2 de l'article 2 de la loi du 30 septembre 1986, tant que l'auteur de l'annonce et l'un de ses lecteurs n'ont pas décidé l'un et l'autre de consentir à un dialogue ; que ce dialogue ne peut être entamé par l'accord donné, quand il est nécessaire, par l'annonceur, de consulter sa carte de visite, puisque ces informations ne sont pas élaborées en fonction d'un lecteur déterminé, celui-ci étant alors indéterminable par l'annonceur puisque dissimulé comme lui, sous un « pseudo » susceptible d'être changé à tout moment ; qu'il en est également ainsi du prix demandé pour la prestation, et la Cour constate que le prévenu ne peut critiquer le comportement de l'officier de police judiciaire à qui il est reproché d'avoir immédiatement demandé après la connexion « Combien ? », ce prix étant justement indifférencié ; que c'est donc inexactement qu'il est allégué que le contenu des communications échangées entre l'officier de police chargé de l'enquête et les prostituées utilisant le service 3615 M avait un caractère privé ;

« alors, d'une part, que, dans ses conclusions, la société X faisait valoir que, selon un arrêt du Conseil d'État du 29 mai 1991, les services de téléconvivialité permettant l'échange d'informations ou de messages entre utilisateurs sur le réseau téléphonique, ne constituent pas des services de communication audiovisuelle au sens de la loi du 30 septembre 1986 ; qu'en énonçant le contraire, la cour d'appel a méconnu les dispositions de ladite loi ;

« alors, d'autre part, que constitue une correspondance protégée au sens de l'article 226-15, alinéa 2, du code pénal, tout message émis, transmis ou reçu par voie de télécommunications, adressé par une personne à une autre dénommée ; que tel est le cas des messages échangés entre 2 utilisateurs du service 3615 M qui se sont mis d'accord pour communiquer entre eux, leurs messages étant inaccessibles au public et à l'exploitant du serveur lui-même ; qu'en décidant que les communications échangées entre l'offi-

cier de police judiciaire et un « pseudo » interconnectés n'avaient pas de caractère privé en raison de leur contenu, puisqu'à la demande du premier quant au prix de prétendues prestations, il était répondu un prix « indifférencié » , la cour d'appel a radicalement méconnu les dispositions des textes susvisés » ;

Attendu que, pour écarter la demande d'annulation de la procédure formée par la société X qui soutenait que le « 36-15 M » ne constituait pas un service de communication audiovisuelle, au sens de la loi du 30 septembre 1986, l'arrêt attaqué constate que ce service a bien pour objet de diffuser, à des personnes indifférenciées, des messages dont le contenu ne peut, par définition, être personnel ; que les juges ajoutent qu'il en résulte nécessairement que les annonces ainsi émises ne peuvent avoir le caractère d'une correspondance privée, tant que l'auteur de l'annonce et l'un de ses lecteurs n'ont pas décidé de consentir à un dialogue ; qu'ils en concluent qu'il s'agit bien d'un service de communication audiovisuelle ;

Attendu qu'en cet état, la cour d'appel n'a méconnu aucun des textes invoqués au moyen qui doit, dès lors, être écarté ;

Sur le deuxième moyen de cassation, pris de la violation des articles 100 à 100-7 du code de procédure pénale, défaut de motifs, manque de base légale :

« en ce que l'arrêt attaqué a rejeté l'exception de nullité présentée par la société X, est entré en voie de condamnation du chef de proxénétisme, et l'a condamnée à une peine d'amende ;

« aux motifs que l'officier de police judiciaire chargé de l'enquête s'étant connecté sur le réseau télématique au moyen d'un terminal mis à la disposition du public par l'opérateur de télécommunications, sans modification préalable de l'utilisation ou du réseau, afin de lire comme n'importe quel utilisateur les annonces offertes par 3615 M, il n'a pu y avoir interception et c'est vainement qu'il est allégué par la défense que les dispositions des articles 100 à 100-7 du code de procédure pénale devaient recevoir application ;

« alors que constitue une interception de correspondances émises par la voie des télécommunications le fait, pour un officier de police judiciaire, dissimulant sa qualité sous un pseudonyme, de prendre contact avec des utilisateurs d'un service télématique et de capter les messages émis par ces correspondants en photographiant l'image du terminal qu'il utilise ; qu'en énonçant le contraire, et en refusant de constater la nullité de l'enquête préliminaire, la cour d'appel a méconnu les dispositions des articles susvisés » ;

Attendu que, pour déclarer irrecevable l'exception proposée par la société X, qui demandait l'annulation d'interceptions de communications émises par la voie télématique, opérées par la police en méconnaissance, selon le prévenu, des articles 100 et suivants du code de procédure pénale, l'arrêt attaqué constate que l'enquêteur s'est connecté au réseau au moyen d'un terminal mis à la disposition du public par l'opérateur, sans modification préalable de l'installation et a lu, comme n'importe quel utilisateur, les an-

nonces offertes par « 3615 M » ; que les juges en concluent qu'il n'y a pas eu interception, au sens des articles précités ;

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

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

Tribunal de grande instance de Paris. 17e Chambre – Chambre de la Presse

Jugement du 2 novembre 2000
Atteinte au secret ou suppression de correspondance par personne dépositaire de l'autorité publique ou chargée de mission de service public, courrier électronique

Motifs

(...) L'article 432-9 du code pénal incrimine 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 et étend cette incrimination, en son alinéa 2, au fait, pour une personne visée ci-dessus 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 télécommunication, d'ordonner, de commettre, ou de faciliter, dans les mêmes conditions, l'interception ou le détournement de correspondances émises, transmises, ou reçues par la voie des télécommunications, ou l'utilisation ou la divulgation de leur contenu.

La commission de cette infraction suppose, outre l'élément légal, la réunion d'un élément matériel et d'un élément intentionnel.

Sur l'élément matériel

L'élément matériel est caractérisé au regard de la qualité de l'auteur de l'infraction, de l'objet de l'infraction, ou de la nature de l'objet protégé, et des actes délictueux incriminés.

– La personne désignée par le texte susvisé doit, d'une part, être dépositaire de l'autorité publique ou chargée d'une mission de service public et, d'autre part, avoir agi dans l'exercice de ses fonctions.

La personne dépositaire de l'autorité publique est celle qui est titulaire d'un pouvoir de décision et de contrainte sur les individus et les choses dont elle use dans l'exercice des fonctions desquelles elle est investie par délégation

de la puissance publique, tandis que la personne chargée d'une mission de service public est celle qui, sans avoir reçu un pouvoir de décision ou de commandement découlant de l'autorité publique, est chargée d'accomplir des actes ou d'exercer une fonction dont la finalité est de satisfaire à un intérêt général.

En l'espèce, X., chercheur au CNRS et directeur du laboratoire..., Y, ingénieur d'études au CNRS et administrateur du système informatique du même laboratoire, et Z., fonctionnaire de la Ville de Paris et maître de conférence au dit laboratoire, ouvrent tous trois au sein de l'École... placée sous la double tutelle du CNRS et de la Ville de PARIS.

Ce faisant, ils sont indéniablement chargés d'une mission de service public d'enseignement dans l'intérêt de la collectivité, ce que, d'ailleurs, ils ne contestent pas.

De même, il apparaît que les reproches qui leur sont faits concernent des actes qu'ils ont accomplis dans l'exercice de cette mission, puisqu'il leur est fiat grief d'avoir mis à profit leur maîtrise du réseau informatique du laboratoire... pour procéder à des investigations dans la messagerie électronique de T., en commettant ainsi un abus de pouvoir.

Dès lors, les dispositions de l'article 432-9 du code pénal leur sont applicables.

– l'objet de l'infraction visée aux termes de ce texte est constitué, soit de correspondances écrites, soit de celles échangées par voie de télécommunications.

En l'espèce, il résulte, à l'évidence, de l'information et des débats que, bien que la présente poursuite soit fondée sur les dispositions de l'alinéa 1 de l'article 432-9 du code pénal, les messages incriminés par la partie civile doivent être analysés comme étant susceptibles d'être des correspondances échangées par voie de télécommunications, dont la violation est prévue et réprimée par l'alinéa 2 du même texte.

En effet, on entend par télécommunication « toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de renseignements de toute nature par fil optique, radio électricité ou autre système électromagnétique », conformément à la définition qu'en donne l'article F32 du code des postes et télécommunications.

Cette énumération inclut toutes les communications à distance actuellement connues, qu'il s'agisse des communications téléphoniques, ou de celles effectuées par minitel, par télécopie, par fax et par satellite réseau internet

Le réseau mondial du Net et l'intégralité des services qu'il offre, comme celui de la messagerie électronique, entrent donc dans le champ d'application de la législation relative aux télécommunications.

Il apparaît, par ailleurs, que le terme correspondance désigne toute relation par écrit existant entre deux personnes identifiables, qu'il s'agisse de lettres, de messages ou de plis fermés ou ouverts.

Cette relation est protégée par la loi, dès lors que le contenu qu'elle véhicule est exclusivement destiné par une personne dénommée à une autre personne également individualisée, à la différence des messages mis à disposition du public.

Le secret en est aménagé suivant les dispositions figurant dans le code pénal sous ses articles 226-13 et 432-9, lesquels reprennent, pour ce qui concerne les télécommunications, la règle posée aux termes du premier alinéa de l'article 1 de la loi du 10 juillet 1991, qui édicte que « le secret des correspondances émises par la voie des télécommunications est garanti par la loi ».

Ces dispositions consacrent, en droit interne, le principe que rappelle l'article 8 de la Convention européenne des droits de l'Homme et des libertés fondamentales, selon lequel la correspondance est un attribut de la vie privée qui justifie la protection légale dont elle est l'objet.

En l'espèce, il convient de déterminer si la messagerie de T. se trouvait protégée par le secret de la correspondance.

Il est nécessaire de rappeler, à ce sujet, que la messagerie électronique permet de transmettre un message écrit d'une personne à une autre, de manière analogue au courrier.

Chacune des personnes désireuses d'effectuer une transmission doit, à cette fin, posséder une adresse électronique dont les deux composantes – son nom et celui de l'entité à laquelle elle est rattachée – définissent son identité informatique, qui est unique. À partir de là, l'une d'elle peut adresser à l'autre tout message qu'elle souhaite lui faire parvenir, son correspondant consultant alors sa boîte aux lettres – dont l'accès peut être protégé par un mot de passe – afin d'y lire les communications qui y ont été envoyées et s'y trouvent en attente.

Le message ainsi transmis revêt les caractéristiques suivantes :
– il est exclusivement destiné à une personne physique ou morale ;
– il s'adresse à une personne individualisée, si son adresse est nominative ; ou déterminée, si son adresse est fonctionnelle, le destinataire final du message n'étant pas précisé en ce cas, mais son récepteur ayant qualité pour recevoir le dit message ;
– il est personnalisé en ce qu'il établit une relation entre l'expéditeur et le récepteur, laquelle fait référence à l'existence d'un lien les unissant qui peut être familial, amical, professionnel ; associatif, etc.

Il en résulte que l'envoi de message électronique de personne à personne constitue de la correspondance privée.

Il convient donc de considérer que la messagerie électronique de la partie civile, à laquelle il n'était, en l'occurrence, possible d'accéder qu'en utilisant son mot de passe, était protégée par le secret de la correspondance émise par voie de télécommunications, dont la violation tombe sous le coup de la loi pénale.

Il importe peu, à cet égard, que l'un des messages dont T. a été destinataire ait été ultérieurement publié dans la presse ou diffusé sur internet, dès lors qu'il lui avait été, au préalable, adressé personnellement, le caractère privé, et donc confidentiel, de cette correspondance résultant de la nature même de cet envoi.

– Les actes délictueux incriminés par l'article 432-9 alinéa 2 du code pénal consistent à intercepter ou détourner des correspondances émises, transmises, ou reçues par la voie des télécommunications ou encore à utiliser ou divulguer des communications interceptées ou détournées par autrui. Le mode opératoire tient au fait de commettre, d'ordonner ou de faciliter ces actes.

En l'espèce, il n'est pas contestable, ni d'ailleurs contesté, que Y et Z. ont intercepté – c'est-à-dire pris connaissance par surprise – certains des messages personnels adressés à T. et contenus dans sa messagerie électronique (...)

(...) Enfin, X. n'a pas dénié avoir donné à ses deux collaborateurs des ordres précis tendant à l'interception des courriers destinés à T (...)

Sur l'élément intentionnel

L'élément intentionnel s'entend, au sens de l'article 432-9 du code pénal, de la volonté des auteurs de l'infraction de commettre les actes délictueux qui y participent, lesquels sont l'interception, ou le détournement de correspondances par voie de télécommunications, ou encore l'utilisation, ou la divulgation de leur contenu.

Cette volonté est manifestée par le comportement de l'auteur du délit qui, ayant connaissance de ce que la correspondance litigieuse ne lui est pas destinée, s'en empare, ou s'informe de son contenu à l'insu de son destinataire.

Si la mauvaise foi n'est pas expressément requise ici, contrairement à ce qui est exigé par la loi pour ce qui est de l'infraction prévue et définie à l'article 226-15 du code pénal qui concerne les mêmes faits délictueux commis par des particuliers, il demeure que l'intention délictueuse de l'auteur ne peut être retenue que dans la mesure où elle s'est clairement exprimée au travers de ses actes.

Enfin, l'intention coupable est indépendante des mobiles auxquels l'auteur prétendait avoir obéi (...)

(...) Les prévenus invoquent, au soutien de leur absence d'intention coupable, le fait que le comportement de T., lequel utilisait abusivement, à des fins privées, la messagerie dont il disposait, au mépris des obligations mises à charge par la charte RENATER – d'où il résulte que les utilisateurs du réseau s'obligent à un usage strictement professionnel –, constituait un cas de force majeure qui légitimait leur intervention dans la messagerie de l'intéressé, dans la mesure où son utilisation abusive du réseau du laboratoire, mettait en cause la sécurité de son système informatique.

Outre que ces circonstances ne constituent pas les cas légaux prévus au texte de l'article 432-9 du code pénal, qui concernent les interceptions faites pour

les nécessités d'une bonne administration de la justice, ou celles dites de sécurité, ou encore celles tombant sous le coup de dispositions légales particulières (postales, douanières ou en rapport avec le fonctionnement des établissements pénitentiaires.

(...) Le souci de la sécurité du système informatique du laboratoire... que Y, Z et X. invoquent pour légitimer les interceptions qu'ils ont commises ou ordonnées n'est donc pas à l'origine de celles-ci et ne saurait les excuser.

Il apparaît, au contraire, que le mobile ayant inspiré leurs actes tient à la recherche de la lettre écrite et signée au lieu et place de... ainsi que Y l'a admis au cours de l'information, et, au-delà, à la volonté de limiter les conséquences que l'antagonisme existant entre la jeune femme et la partie civile était susceptible d'engendrer pour l'établissement.

Les prévenus doivent, au vu de l'ensemble de ces éléments, être déclarés coupables des faits qui leur sont reprochés.

Jurisprudence de la Cour européenne des droits de l'Homme

Cour européenne des droits de l'Homme

Affaire Amann c. Suisse
Arrêt du 16 février 2000

Résumé des données de l'affaire

– Les faits

Le requérant Hermann Amann importait des appareils dépilatoires dont il faisait la publicité dans des magazines. Le 12 octobre 1981, une femme lui téléphona de l'ambassade alors soviétique à Berne pour commander un appareil dépilatoire « Perma Tweez ». Cet appel téléphonique fut intercepté par le ministère public de la Confédération, lequel demanda au service des renseignements de la police du canton de Zurich d'enquêter sur le requérant. Sur la base du rapport établi par la police zurichoise, le ministère public rédigea en décembre 1981 pour son fichier destiné à assurer la protection de l'État une fiche sur le requérant. En particulier, ladite fiche indiquait que le requérant avait été « identifié comme contact auprès de l'ambassade russe » et était commerçant ; elle portait le numéro (1153 : 0) 614, ce code signifiant « pays à régime communiste » (1), « Union soviétique » (153), « espionnage établi » (0) et « divers contacts avec le bloc de l'Est » (614). En 1990, le requérant eut vent de l'existence du fichier du ministère public et demanda à consulter sa fiche. Il en obtint une photocopie en septembre 1990 –, toutefois, deux passages avaient été cancelés.

– La procédure

Après avoir vainement tenté d'obtenir la divulgation des passages caviardés, le requérant saisit le Tribunal fédéral d'une action de droit administratif, sollicitant notamment de la Confédération une réparation d'un montant de 5 000 francs suisses pour avoir été irrégulièrement fiché par le ministère public. Par un arrêt du 14 septembre 1994, notifié le 25 janvier 1995, se référant aux articles 66 et suivants, en particulier 72 PPF, relatifs à la surveillance des communications téléphoniques et de la correspondance postale, ainsi que 265 et suivants du code pénal, régissant les « crimes ou délits contre l'État », le Tribunal fédéral rappela qu'il était admissible – avant même que des poursuites ne fussent engagées – de recueillir des informations afin de prévenir des infractions contre l'État ou la défense nationale, si des éléments donnaient à penser que les préparatifs d'une telle infraction étaient en cours et rejeta cette demande, au motif que le requérant n'avait pas subi d'atteinte grave à sa personnalité.

Le requérant a saisi la Commission au motif que l'interception de l'appel téléphonique du 12 octobre 1981 de même que l'établissement par le ministère public de la fiche le concernant et la conservation de cette dernière dans le fichier de la Confédération ont méconnu l'article 8 de la Convention européenne des droits de l'Homme. Il se plaint en outre de n'avoir pas bénéficié d'un recours effectif, au sens de l'article 13 de la Convention, pour faire redresser les violations alléguées. La Commission a retenu sa requête le 3 décembre 1997 et estimé dans son rapport du 20 mai 1998 qu'il y a eu violation de l'article 8, mais pas de l'article 13. L'affaire a été en conséquence déférée à la Cour Européenne des Droits de l'Homme.

Extraits de l'arrêt

(...) I – SUR LA VIOLATION ALLÉGUÉE DE L'ARTICLE 8 DE LA CONVENTION QUANT A L'INTERCEPTION DE L'APPEL TELEPHONIQUE DU 12 OCTOBRE 1981

(...)

A – Applicabilité de l'article 8

44. La Cour rappelle que les appels téléphoniques reçus dans des locaux privés ou professionnels sont compris dans les notions de « vie privée » et de « correspondance » visée à l'article 8 § 1 (arrêt Halford c. Royaume Uni). Ce point n'a d'ailleurs pas prêté à controverse.

B – Observations de l'article 8

1. Sur l'existence d'une ingérence

45. La Cour note qu'il n'est pas contesté que le ministère public a intercepté et enregistré un appel téléphonique reçu par le requérant le 12 octobre 1981 d'une personne de l'ambassade alors soviétique à Berne. Il y a donc eu « ingérence d'une autorité publique », au sens de l'article 8 § 2, dans l'exercice d'un droit garanti au requérant par le paragraphe 1 de cette disposition (arrêt Kopp c. Suisse).

2. Justification de l'ingérence

46. Pareille ingérence méconnaît l'article 8 sauf si, « prévue par la loi », elle poursuit un ou des buts légitimes au regard du paragraphe 2 et, de surcroît, est nécessaire dans une société démocratique pour atteindre ces derniers.

a) L'ingérence était-elle « prévue par la loi » ?

47. D'après le requérant, la base en droit suisse fait défaut. En particulier, il affirme que la mesure litigieuse ne peut pas se fonder sur les articles 66 à 72 PPF, le Gouvernement n'ayant produit aucun élément susceptible de prouver qu'une poursuite pénale avait été ouverte contre un tiers ou que les autorités s'étaient conformées à la procédure fixée par ces dispositions. À cet égard, il souligne que l'allégation du Gouvernement selon laquelle les documents ne seraient plus disponibles n'est pas crédible.

En effet, il ressort du rapport de la commission d'enquête parlementaire en charge d'instruire l'affaire dite des fiches qu'il existe des listes relatives aux écoutes téléphoniques ordonnées par le ministère public qui sont exécutées par les PTT ; par ailleurs, la chambre d'accusation du Tribunal fédéral possède les registres dans lesquels sont consignées les autorisations délivrées par son président ; de surcroît, le Gouvernement ne peut prétendre qu'un employé de l'ambassade alors soviétique à Berne était surveillé que s'il dispose de documents pour étayer cette affirmation ; enfin, le fait que l'enregistrement n'a pas été détruit « à l'issue de la procédure » (article 66 § 1 ter PPF) démontre qu'il n'y avait pas d'instruction au sens des articles 66 et suivants PPF.

Le requérant exprime l'avis que l'ensemble des lignes téléphoniques de l'ambassade alors soviétique à Berne étaient écoutées de façon systématique, en dehors de tout soupçon concret contre une personne déterminée et d'une procédure judiciaire conforme à la loi. Selon lui, cette présomption est confirmée par le fait qu'au cours de la procédure devant les autorités suisses, celles-ci ont expressément mentionné les termes « informations de contre-espionnage ». En outre, les enquêtes de la commission d'enquête parlementaire en charge d'instruire l'affaire dite des fiches ont démontré que les organes de la police fédérale avaient surveillé les citoyennes et citoyens pendant des décennies sans autorisation de la part d'un tribunal. Or l'article 17 § 3 PPF ne saurait fonder de tels procédés de la police politique.

Quant à l'arrêté du Conseil fédéral du 29 avril 1958 concernant le Service de police du ministère public fédéral, le requérant souligne que ce texte contient des dispositions purement organisationnelles relatives aux différents offices du Département fédéral de justice et de police et ne donne aucunement pouvoir à ces derniers de s'ingérer dans des droits et libertés protégés par la Convention ; il ne peut dès lors être considéré comme une base légale adéquate. Au demeurant, le requérant considère que ce texte n'est pas suffisamment précis et accessible pour satisfaire à l'exigence de « prévisibilité » telle que définie par la jurisprudence de la Cour.

48. Pour la commission, la surveillance de l'entretien téléphonique du requérant ne repose pas sur une base légale suffisante. En effet, l'arrêté du Conseil fédéral du 29 avril 1958 concernant le Service de police du ministère public fédéral est rédigé en termes trop généraux. Par ailleurs, il n'a pas été démontré que la procédure prévue aux articles 66 et suivants PPF avait été suivie.

49. Le Gouvernement soutient que l'existence d'une base légale en droit suisse ne fait aucun doute. À titre préliminaire, il indique que la mesure litigieuse a été effectuée dans le cadre d'une surveillance décidée par le ministère public à l'encontre d'un collaborateur déterminé de l'ambassade alors soviétique à Berne, en application de l'article 66 § 1 bis PPF, et que le requérant n'était pas la personne visée par la mise sur écoute, ni en qualité de suspect ni en qualité de tiers (ce dernier étant la personne ayant commandé l'appareil dépilatoire) ; le requérant a donc été enregistré « par hasard », en qualité de « participant nécessaire ».

Pour le Gouvernement, il importe peu de savoir si la mesure litigieuse a été décidée dans le cadre d'une procédure pénale déjà engagée ou dans le but de prévenir une infraction puisque les articles 17 § 3 (fondé sur l'article 102 §§ 9 et 10 de la Convention fédérale) et 72 PPF ainsi que 1er de l'arrêté du Conseil fédéral du 29 avril 1958 concernant le Service de police du ministère public fédéral constituent une base légale suffisante dans les deux hypothèses. Il souligne que la Cour, dans une affaire similaire, a conclu à l'existence d'une base légale en droit suisse (arrêt Kopp précité).

La seule question décisive est celle de savoir si les garanties fixées par la loi ont été respectées. À cet égard, le Gouvernement déclare que, dans l'impossibilité d'avoir accès au dossier, il ne peut vérifier si l'approbation du président de la chambre d'accusation du Tribunal fédéral requise par l'article 66 bis PPF a été accordée. Sur la base du rapport établi par la commission d'enquête parlementaire en charge d'instruire l'affaire dite des fiches, aux termes duquel le président de la chambre d'accusation du Tribunal fédéral avait approuvé toutes les décisions du juge d'instruction, il suppose toutefois que tel a été le cas en l'espèce.

50. La Cour rappelle sa jurisprudence constante selon laquelle les mots « prévue par la loi » imposent non seulement que la mesure incriminée ait une base en droit interne, mais visent aussi la qualité de la loi en cause : ainsi, celle-ci doit être accessible au justiciable et prévisible (arrêt Kopp).

(...) 52. La Cour rappelle qu'il incombe au premier chef aux autorités nationales, et singulièrement aux tribunaux d'interpréter et d'appliquer le droit interne (arrêt Kruslin c. France et Kopp précité). À cet égard, elle relève que dans son arrêt du 14 septembre 1994, le Tribunal fédéral a estimé qu'il n'était pas nécessaire de rechercher si les articles 17 § 3 PPF et 1 er de l'arrêté du Conseil fédéral du 29 avril 1958 concernant le service de police du ministère public fédéral étaient susceptibles de justifier l'atteinte à la personnalité alléguée par le requérant. Par ailleurs, cette juridiction ne s'est exprimée qu'en des termes très généraux sur l'article 72 PPF, se limitant à

rappeler qu'il était admissible de recueillir des informations afin de prévenir des infractions contre l'État ou la défense nationale lorsque des éléments donnaient à penser que les préparatifs d'une telle infraction étaient en cours.

53. Il est vrai que la Cour s'est déjà prononcée sur la question de savoir si la loi fédérale sur la procédure pénale constituait, en droit suisse, une base légale suffisante en matière d'écoutes téléphoniques (arrêt Kopp). À la différence de la présente affaire, toutefois, l'autorité alors saisie par M Kopp (le Conseil fédéral) avait examiné de manière détaillée la question de la légalité de la surveillance et l'article 72 PPF n'était pas en cause.

54. En l'espèce, la Cour n'estime pas nécessaire de rechercher si l'interception de l'appel téléphonique du 12 octobre 1981 reposait sur une base légale. En effet, à supposer même que tel fût le cas, l'une des exigences découlant de l'expression « prévue par la loi », en l'occurrence la prévisibilité, ne se trouve pas réalisée.

ii. Qualité de la loi

55. La Cour rappelle que les mots « prévue par la loi » impliquent des conditions qui vont au-delà de l'existence d'une base légale en droit interne et exigent que celle-ci soit « accessible » et « prévisible ».

56. Selon la jurisprudence constante de la Cour, une norme est « prévisible » lorsqu'elle est rédigée avec assez de précision pour permettre à toute personne, en s'entourant au besoin de conseils éclairés, de régler sa conduite (arrêt Malone c. Royaume Uni). En matière de mesures de surveillance secrète, la Cour a souligné l'importance de ce concept en ces termes :

« La Cour rappelle qu'à ses yeux le membre de phrase « prévue par la loi » ne se borne pas à renvoyer au droit interne, mais concerne aussi la qualité de la « loi » ; il la veut compatible avec la prééminence du droit, mentionné dans le préambule de la Convention (). Il implique ainsi – et cela ressort de l'objet et du but de l'article 8 – que le droit interne doit offrir une certaine protection contre des atteintes arbitraires de la puissance publique aux droits garantis par la paragraphe 1 (). Or le danger d'arbitraire apparaît avec une netteté singulière là où un pouvoir de l'exécutif s'exerce en secret (...)

(...) Puisque l'application de mesures de surveillance secrète des communications échappe au contrôle des intéressés comme du public, la « loi » irait à l'encontre de la prééminence du droit si le pouvoir d'appréciation accordé à l'exécutif ne reconnaissait pas de limites. En conséquence, elle doit définir l'étendue et les modalités d'exercice d'un tel pouvoir avec uns netteté suffisante – compte tenu du but légitime poursuivi – pour fournir à l'individu une protection adéquate contre l'arbitraire » .

Elle a aussi précisé que les écoutes et autres formes d'interceptions 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 (arrêt Kopp).

57. Il convient donc d'examiner la « qualité » des normes juridiques invoquées en l'espèce.

58. La Cour relève d'abord que l'article 1er de l'arrêté du Conseil fédéral du 29 avril 1958 concernant le service de police du ministère public fédéral, aux termes duquel la police fédérale « assure le service des enquêtes et des informations dans l'intérêt de la sûreté intérieure et extérieure de la Confédération » notamment par des mesures de « surveillance », ne contient aucune indication relative aux personnes susceptibles de faire l'objet de telles mesures, aux circonstances dans lesquelles celles-ci peuvent être ordonnées, aux moyens à employer ou aux procédures à observer. Cette norme ne saurait en conséquence être considérée comme suffisamment claire et détaillée pour assurer une protection appropriée contre les ingérences des autorités dans le droit du requérant au respect de sa vie privée et de sa correspondance.

59. Elle estime qu'il en est de même de l'article 17 § 3 PPF, rédigé en des termes similaires.

60. Quant aux autres dispositions de la loi fédérale sur la procédure pénale, elle observe que l'article 66 définit les catégories de personnes susceptibles d'être mises sur écoutes judiciaires ainsi que les circonstances dans lesquelles une telle surveillance peut être ordonnée. Par ailleurs, les articles 66 bis et suivants fixent la procédure à suivre ; ainsi, l'exécution de la mesure est limitée dans le temps et soumise au contrôle d'un magistrat indépendant, en l'occurrence le président de la chambre d'accusation du Tribunal fédéral.

61. La Cour ne minimise nullement la valeur de ces garanties. Toutefois, elle souligne que le Gouvernement n'a pas été en mesure d'établir que les conditions d'application de l'article 66 PPF avaient été respectées et les mécanismes de protection prévus aux articles 66 et suivants PPF observés.

Elle relève en outre qu'au dire du Gouvernement, le requérant n'était pas la personne visée par la mesure litigieuse, ni en qualité de suspect ou d'inculpé ni en qualité de tiers présumé recevoir ou transmettre des informations à un suspect ou un inculpé, mais a participé « par hasard » à une conversation téléphonique enregistrée dans le cadre d'une surveillance dirigée contre un collaborateur déterminé de l'ambassade alors soviétique à Berne.

Or la loi fédérale sur la procédure pénale vise avant tout la surveillance des personnes suspectées ou inculpées d'un crime ou d'un délit (article 66 § 1 PPF), voire les tiers présumés recevoir ou transmettre des informations à ces dernières (article 66 § 1 bis PPF), mais ne réglemente pas de façon détaillée le cas des interlocuteurs écoutés « par hasard », en qualité de « participants nécessaires » à une conversation téléphonique enregistrée par les autorités en application de ces dispositions. En particulier, la loi ne précise pas les précautions à prendre à leur égard.

62. La Cour conclut que l'ingérence ne saurait passer pour « prévue par la loi » puisque le droit suisse n'indique pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine considéré.

Il s'ensuit qu'il y a eu violation de l'article 8 de la Convention en ce qui concerne l'enregistrement de l'appel téléphonique reçu par le requérant le 12 octobre 1981 d'une personne de l'ambassade alors soviétique à Berne.

b) Finalité et nécessité de l'ingérence

63. Eu égard à la conclusion qui précède, la Cour n'estime pas nécessaire d'examiner le respect des autres exigences du paragraphe 2 de l'article 8.

II. SUR LA VIOLATION ALLÉGUÉE DE L'ARTICLE 8 DE LA CONVENTION QUANT A L'ÉTABLISSEMENT D'UNE FICHE ET SA CONSERVATION DANS LE FICHIER DE LA CONFÉDÉRATION

64. Le requérant se plaint de ce que l'établissement d'une fiche le concernant à la suite de l'interception de l'appel téléphonique reçu d'une personne de l'ambassade alors soviétique à Berne, et sa conservation dans le fichier de la Confédération, ont entraîné une violation de l'article 8 de la Convention.

A. Applicabilité de l'article 8

65. La Cour rappelle que la mémorisation de données relatives à la « vie privée » d'un individu entre dans le champ d'application de l'article 8 § 1 (arrêt Leander c. Suède).

À cet égard, elle souligne que le terme « vie privée » ne doit pas être interprété de façon restrictive. En particulier, le respect de la vie privée englobe le droit pour l'individu de nouer et développer des relations avec ses semblables ; de surcroît, aucune raison de principe ne permet d'exclure les activités professionnelles ou commerciales de la notion de « vie privée » (arrêt Niemietz c. Allemagne).

Cette interprétation extensive concorde avec celle de la Convention élaborée au sein du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, entrée en vigueur le 1er octobre 1985, dont le but est « de garantir, sur le territoire de chaque partie, à toute personne physique (...) le respect de ses droits et libertés fondamentaux, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant » (article 1), ces dernières étant définies comme « toute information concernant une personne physique identifiée ou identifiable » (article 2).

66. En l'espèce, la Cour relève qu'une fiche a été établie concernant le requérant, sur laquelle il a été indiqué que ce dernier était un « contact auprès de l'ambassade russe » et faisait « du commerce de différentes sortes avec la société [A.] » (voir les paragraphes 15 et 18 ci-dessus).

67. Pour la Cour, il s'agit là sans contredit de données relatives à la « vie privée » du requérant et l'article 8 trouve en conséquence à s'appliquer à ce grief également.

B. Observation de l'article 8

1. Sur l'existence d'une ingérence

68. Pour le Gouvernement, la question de savoir s'il y a eu « ingérence » au sens de l'article 8 de la Convention demeure posée, puisque « la fiche ne contenait aucun élément sensible en rapport avec la vie privée du requérant », que ce dernier « n'a subi aucun inconvénient du fait de l'établissement et de la conservation de la fiche » et que celle-ci n'a « très probablement jamais été consultée par des tiers ».

69. La Cour rappelle que la mémorisation par une autorité publique de données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8. L'utilisation ultérieure des informations mémorisées importe peu (voir, mutatis mutandis, arrêts Leander précités).

70. En l'espèce, la Cour relève qu'une fiche contenant des données relatives à la vie privée du requérant a été établie par le ministère public, puis conservée dans le fichier de la Confédération. À cet égard, elle souligne qu'il ne lui appartient pas de spéculer sur le caractère sensible ou non des éléments recueillis ni sur les éventuels inconvénients subis par le requérant. Il lui suffit de constater que des données relatives à la vie privée d'un particulier ont été mémorisées par une autorité publique pour conclure qu'en l'espèce, l'établissement et la conservation de la fiche litigieuse constituent une ingérence, au sens de l'article 8, dans le droit au respect de la vie privée du requérant.

2. Justification de l'ingérence

71. Pareille ingérence méconnaît l'article 8 sauf si, « prévue par la loi », elle poursuit un ou des buts légitimes au regard du paragraphe 2 et, de surcroît, est nécessaire dans une société démocratique pour atteindre ces derniers.

a) L'ingérence était-elle « prévue par la loi » ?

72. Selon le requérant, l'établissement et la conservation de la fiche le concernant sont des mesures qui ne reposent pas sur une base légale. En particulier, il affirme que l'article 17 § 3 PPF n'autorise pas la police fédérale à consigner les résultats de ses mesures de surveillance. Quant aux directives du Conseil fédéral du 16 mars 1981 applicables au traitement des données personnelles dans l'administration fédérale, elles sont destinées aux fonctionnaires de l'administration et il ne s'agit donc pas d'une loi suffisamment claire et précise pour permettre aux citoyens de déterminer leurs droits et obligations.

Il soutient que de surcroît, les autorités ne se sont pas conformées aux normes en vigueur, puisque l'article 66 § 1 ter PPF et le chiffre 414 des directives du Conseil fédéral du 16 mars 1981 applicables au traitement des

données personnelles dans l'administration fédérale exigeaient la destruction des enregistrements ne s'avérant pas nécessaires pour l'exécution d'une enquête.

Enfin, il souligne que la législation entrée en vigueur au début des années 90, après l'éclatement de l'affaire dite des fiches, ne prévoit pas la possibilité d'engager une procédure judiciaire aux fins d'obtenir la destruction d'une fiche. Ainsi, aux termes de l'arrêté fédéral du 9 octobre 1992 sur la consultation des documents du ministère public de la Confédération et de l'ordonnance du Conseil fédéral du 20 janvier 1993 sur la consultation des documents du ministère public de la Confédération, les fiches sont conservées dans les archives fédérales et il est seulement loisible aux justiciables d'y faire annoter une remarque lorsque le contenu en est contesté.

73. La Commission partage l'opinion du requérant. En particulier, elle estime que les directives du Conseil fédéral du 16 mars 1981 applicables au traitement des données personnelles dans l'administration fédérale ne sont pas assez précises et se contentent de présupposer, sans en donner une elles-mêmes, une base légale à la mémorisation d'informations.

74. Le Gouvernement soutient que l'ordre juridique suisse offre, compte tenu « des particularités caractérisant les mesures secrètes dans le domaine de la protection de la sécurité de l'État », une base légale suffisamment accessible et prévisible.

Il est d'avis qu'avant 1990, les mesures litigieuses étaient principalement fondées sur les articles 17 § 3 PPF et 1 er de l'arrêté du Conseil fédéral du 29 avril 1958 concernant le Service de police du ministère public fédéral, ces dispositions étant concrétisées par les directives du Conseil fédéral du 16 mars 1981 applicables au traitement des données personnelles dans l'administration fédérale. Il précise que ces directives ont été publiées. (...)

Après 1990, plusieurs textes ont été édictés en matière de traitement et de consultation de documents contenant des données personnelles, en particulier l'ordonnance du Conseil fédéral du 5 mars 1990 relative au traitement des documents de la Confédération établis pour assurer la protection de l'État, l'arrêté fédéral du 9 octobre 1992 sur la consultation des documents du ministère public de la Confédération et l'ordonnance du Conseil fédéral du 20 janvier 1993 sur la consultation des documents du ministère public de la Confédération.

i. L'établissement de la fiche

75. La Cour relève qu'en décembre 1981, date à laquelle fut établie la fiche concernant le requérant, la loi fédérale sur la procédure pénale, l'arrêté du Conseil fédéral du 29 avril 1958 concernant le Service de police du ministère public fédéral et les directives du Conseil fédéral du 16 mars 1981 applicables au traitement des données personnelles dans l'administration fédérale étaient en vigueur. Toutefois, aucun de ces textes ne mentionnant expressément l'existence d'un registre du ministère public, la question pourrait se poser de savoir si la rédaction de la fiche litigieuse reposait sur

« une base légale en droit suisse » et, dans l'affirmative, si cette dernière était « accessible » (arrêt Leander précité). À cet égard, elle observe en effet que les directives du Conseil fédéral du 16 mars 1981 étaient avant tout destinées au personnel de l'administration fédérale.

En l'espèce, cependant, elle n'estime pas nécessaire de se prononcer à ce sujet, puisqu'à supposer même que l'établissement de la fiche, en décembre 1981, fût fondé sur une base légale accessible, celle-ci n'était pas « prévisible ».

76. La Cour a jugé ci-dessus (paragraphes 58 et 59) que les articles 17 § 3 PPF et 1er de l'arrêté du Conseil fédéral du 29 avril 1958 concernant le Service de police du ministère public fédéral étaient rédigés en termes trop généraux pour satisfaire à l'exigence de prévisibilité en matière d'écoutes téléphoniques. Pour les motifs déjà exposés, elle aboutit à la même conclusion concernant la création de la fiche sur le requérant.

Quant aux directives du Conseil fédéral du 16 mars 1981 applicables au traitement des données personnelles dans l'administration fédérale, elles énoncent quelques principes généraux, par exemple que le « traitement de données personnelles doit reposer sur une base légale » ou que les « données personnelles ne doivent être traitées que dans des buts bien déterminés », mais ne contiennent aucune indication appropriée sur l'étendue et les modalités d'exercice du pouvoir conféré au ministère public de recueillir, enregistrer et conserver des informations ; ainsi, elles ne précisent pas les conditions d'établissement des fiches, les procédures à suivre, les informations pouvant être mémorisées et les mentions éventuellement interdites.

Ces directives, à l'instar de la loi fédérale sur la procédure pénale et l'arrêté du Conseil fédéral du 29 avril 1958 concernant le Service de police du ministère public fédéral, ne sauraient en conséquence être considérées comme suffisamment claires et détaillées pour assurer une protection adéquate contre les ingérences des autorités dans le droit du requérant au respect de sa vie privée.

77. L'établissement de la fiche concernant le requérant n'était donc pas « prévu par la loi » au sens de l'article 8 de la Convention.

ii. La conservation de la fiche

78. La Cour souligne d'abord qu'il paraît douteux que la conservation d'une fiche dont la création n'a pas été « prévue par la loi » puisse satisfaire à cette exigence.

De surcroît, elle relève que le droit suisse et ce, tant avant qu'après 1990, prévoit expressément la destruction des données qui ne s'avèrent plus « nécessaires » ou sont devenues « inutiles » (article 66 § 1 ter PPF, chiffre 414 des directives du Conseil fédéral du 16 mars 1981 applicables au traitement des données personnelles dans l'administration fédérale et article 7 de l'arrêté fédéral du 9 octobre 1992 sur la consultation des documents du ministère public de la Confédération).

Or en l'espèce, les autorités n'ont pas détruit les renseignements mémorisés lorsqu'il s'est avéré qu'aucune infraction n'était en cours de préparation, comme le souligne le Tribunal fédéral dans son arrêt du 14 septembre 1994.

79. Pour ces motifs, la conservation de la fiche concernant le requérant n'était pas « prévue par la loi » au sens de l'article 8 de la Convention.

80. La Cour conclut que tant l'établissement de la fiche litigieuse par le ministère public que la conservation de cette dernière dans le fichier de la Confédération constituent des ingérences dans la vie privée du requérant qui ne sauraient passer pour « prévues par la loi » puisque le droit suisse n'indique pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine considéré. Il s'ensuit qu'il y a eu violation de l'article 8 de la Convention.

b) finalité et nécessité de l'ingérence

81. Eu égard à la conclusion qui précède, la Cour n'estime pas nécessaire d'examiner le respect des autres exigences du paragraphe 2 de l'article 8.

III. SUR LA VIOLATION ALLÉGUÉE DE L'ARTICLE 13 DE LA CONVENTION

82. Le requérant allègue en outre une violation de l'article 13 de la Convention, ainsi libellé :

« Toute personne dont les droits et libertés reconnus dans la (...) Convention ont été violés, a droit à l'octroi d'un recours effectif devant une instance nationale, alors même que la violation aurait été commise par des personnes agissant dans l'exercice de leurs fonctions officielles. »

(...)

B. Sur le bien-fondé du grief

(...)

89. En l'espèce, la Cour relève que le requérant a été en mesure de consulter sa fiche dès qu'il en a fait la demande, en 1990, lorsque la population dans son ensemble eut connaissance de l'existence du fichier du ministère public. Elle souligne en outre que le requérant a intenté une action de droit administratif devant le Tribunal fédéral et qu'à cette occasion, il a été en mesure de se plaindre de ce que la surveillance téléphonique et la rédaction de la fiche ne reposaient pas sur une base légale, d'une part, et de l'absence de « recours effectif » contre ces mesures, d'autre part. Elle note que le Tribunal fédéral avait compétence pour se prononcer sur ces griefs et a procédé à leur examen ; à cet égard, elle rappelle que le seul fait que le requérant soit débouté de toutes ses conclusions ne constitue pas en soi un élément suffisant pour juger du caractère « effectif » ou non de l'action de droit administratif.

90. Le requérant a donc disposé, en droit suisse, d'un recours effectif pour exposer les violations de la Convention qu'il alléguait. Partant, il n'y a pas eu violation de l'article 13.

(...)

PAR CES MOTIFS, LA COUR, A L'UNANIMITÉ,

1. Dit qu'il y a eu violation de l'article 8 de la Convention concernant l'interception de l'appel téléphonique ;

2. Dit qu'il y a eu violation de l'article 8 de la Convention concernant l'établissement et la conservation de la fiche ;

3. Rejette l'exception préliminaire du Gouvernement relative à l'article 13 ;

4. Dit qu'il n'y a pas eu violation de l'article 13 de la Convention ;

5. Dit que le présent arrêt constitue en soi une satisfaction équitable suffisante pour le dommage moral subi par le requérant.

Cour européenne des droits de l'Homme

Affaire Jasper c. Royaume Uni
Arrêt du 16 février 2000

Résumé des données de l'affaire

– Les faits

Le requérant, Eric Jasper, a été condamné en 1994 à une peine d'emprisonnement pour importation de cannabis un an auparavant.

Il lui était reproché d'avoir pris possession, transporté dans un camion frigorifique et stocké trois tonnes de drogue dissimulées dans une cargaison de viande congelée. Pour sa défense, il indiquait ne pas avoir su qu'il y avait du cannabis dans la cargaison et que, cherchant à monter une entreprise de transport, il n'avait fait que transporter des marchandises en toute innocence n'ayant agit que sur les instructions téléphoniques d'une autre entreprise de transport.

Peu avant l'ouverture du procès, le juge fut saisi d'une requête unilatérale de l'accusation tendant à voir reconnaître une immunité d'intérêt public la dispensant de communiquer certaines pièces en sa possession. La défense fut avisée qu'une requête allait être introduite mais ne fut pas informée de la catégorie dont relevaient les documents que l'accusation souhaitait ne pas devoir divulguer. Elle se vit donner l'occasion d'exposer au juge les grandes lignes de son argumentation, qui consistait à dire que le requérant avait pris livraison de la cargaison de viande conformément à des instructions reçues par téléphone la nuit précédente et qu'il ignorait que la viande contenait du cannabis, et elle invita le juge à ordonner la divulgation de toute preuve se rapportant à ces faits allégués. Le juge, lors d'une audience non contradictoire, examina les éléments en question et décida qu'ils ne devaient pas être divulgués. La défense ne fut pas informée des motifs étayant cette décision.

La défense présenta à l'accusation quelques jours plus tard la requête écrite suivante :

« 9. Nous demandons formellement à l'accusation de dire a) d'une manière générale, s'il existe, en rapport avec la présente espèce et hormis ceux qui ont fait l'objet de la requête unilatérale présentée au tribunal le vendredi 14 janvier 1994 (...), des éléments non exploités qui n'auraient pas été divulgués, et b) en particulier :

i) si des systèmes d'écoute ou d'interception téléphonique ont été utilisés, et, dans l'affirmative, s'il en existe des enregistrements, des notes, des mémorandums ou d'autres pièces ; (...) »

Le représentant de l'accusation refusa de répondre sur ce point particulier.

Le juge rejeta par la suite une demande de la défense formulée en vue d'enjoindre l'accusation de produire les renseignements demandés.

Devant la cour d'appel, le requérant excipa des motifs suivants :

« Il était clair que l'ensemble des éléments non exploités n'avaient pas été divulgués (...). Il fut déclaré en audience publique au nom de l'accusé que les éléments non exploités pouvaient avoir de l'importance pour sa défense, qu'il ne savait pas si des drogues devaient être ou étaient dissimulées dans la cargaison qu'il transportait, et qu'il avait reçu ses instructions de livraison par téléphone, dans le cadre de son activité de transporteur, très peu de temps avant le 1er juillet 1993 (...). Dès lors, toute information qui aurait pu lui permettre de confirmer la source ou le contenu de ces instructions et d'identifier les personnes qui l'avaient impliqué dans une affaire de contrebande étaient d'une importance manifeste. L'accusation avait refusé de répondre à la question de savoir si, hormis ceux qui faisaient l'objet de la requête unilatérale, elle avait gardé par-devers elle des éléments potentiellement pertinents au motif que leur divulgation aurait permis de déterminer si oui ou non des interceptions téléphoniques avaient eu lieu. Il ressortait clairement du déroulement qu'avait connu le débat que la requête unilatérale n'avait pas traité d'interceptions téléphoniques, l'accusation ayant soutenu que cette question relevait de la compétence exclusive du procureur et non de celle du juge, thèse qui se fondait sur la décision *R. v. Preston* (...). Dans ces conditions, la défense avait le droit de savoir tout au moins quelle catégorie d'éléments n'avait pas fait l'objet de ladite requête (...). De surcroît, l'accusation aurait dû être invitée à justifier, au besoin dans le cadre de la procédure non contradictoire, le point de vue défendu par elle quant aux autres éléments non exploités (...) Dès lors qu'il doit avoir existé un motif d'observer l'accusé – motif qui ne fut expliqué ni par les preuves produites ni par celles communiquées mais exclues d'un commun accord – et dès lors qu'il a été déclaré qu'aucun informateur n'est intervenu en l'espèce, il est très probable que des informations ne pouvant être couvertes par l'immunité d'intérêt public et directement relatives à la cause de l'accusé étaient en possession de l'accusation. »

La cour rejeta le recours.

– La procédure

M. Jasper a saisi la Commission en alléguant que la non-divulgation par l'accusation d'éléments de preuve pertinents jugés couverts par une immunité d'intérêt public l'avait privé d'un procès équitable au sens de l'article 6 §§ 1 et 3 b) et d) de la Convention. La Commission, dans son rapport du 20 octobre 1998, a formulé l'avis qu'il n'y avait pas eu de violation de la Convention. M. Jasper a donc saisi la Cour.

Extraits de l'arrêt

[...] I. SUR LA VIOLATION ALLÉGUÉE DE L'ARTICLE 6 §§ 1 ET 3 b) ET d) DE LA CONVENTION

42. Le requérant allègue que, prises ensemble, les procédures devant la *Crown Court* et la Cour d'appel ont violé les droits à lui garantis par l'article 6 §§ 1 et 3 b) et d) de la Convention, dont les parties pertinentes en l'espèce sont ainsi libellées :

« 1. Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable, par un tribunal indépendant et impartial, établi par la loi, (...)

3. Tout accusé a droit notamment à : (...)

b) disposer du temps et des facilités nécessaires à la préparation de sa défense ; (...)

d) interroger ou faire interroger les témoins à charge et obtenir la convocation et l'interrogation des témoins à décharge dans les mêmes conditions que les témoins à charge ; (...) »

43. Il considère que toute omission de divulguer des preuves pertinentes sape le droit à un procès équitable. Avec le gouvernement et la Commission, il reconnaît que le droit à une divulgation intégrale n'est pas absolu et peut, lorsque sont poursuivis des buts légitimes, tels que la protection de la sécurité nationale, de témoins vulnérables ou de sources d'information, être soumis à des limitations, mais il estime que toute restriction aux droits de la défense doit être strictement proportionnée et assortie de garanties procédurales propres à compenser le handicap infligé à la défense. Tout en admettant que dans certaines circonstances il pourrait être nécessaire, dans l'intérêt public, d'exclure l'accusé et ses représentants de la procédure de divulgation, il soutient que l'audience non contradictoire devant le juge a violé l'article 6 de la Convention, dès lors qu'elle n'offrait aucune garantie contre les préventions ou erreurs judiciaires et qu'il n'y fut pas possible de présenter des arguments au nom de l'accusé.

44. Le requérant estime qu'il était nécessaire, aux fins de l'article 6, de contrebalancer la non-participation de la défense à la procédure par l'introduction d'un élément contradictoire tel que la désignation d'un avocat indépendant qui eût été à même de présenter des arguments pour le compte de la défense quant au caractère pertinent ou non des preuves dissimulées, de

vérifier le bien-fondé de la demande de reconnaissance d'une immunité d'intérêt public présentée par l'accusation et d'agir comme rempart indépendant contre le risque d'erreurs ou de préventions judiciaires. Et de citer quatre cas où une procédure faisant intervenir un avocat spécial a été introduite au Royaume Uni. Ces exemples démontreraient qu'un mécanisme de rechange était disponible qui eût assuré, dans toute la mesure du possible, le respect des droits de la défense dans le cadre d'une audience consacrée à l'examen de la question de savoir si l'intérêt public justifiait la rétention par l'accusation de certains éléments de preuve, tout en prenant en compte des soucis légitimes relatifs, par exemple, à la sécurité nationale ou à la protection de témoins ou de sources d'information, et il incomberait au Gouvernement de démontrer qu'il n'était pas possible en l'espèce d'introduire pareille procédure.

45. Enfin, le requérant soutient que son procès a aussi manqué d'équité en ce que le produit d'une interception téléphonique a été dissimulé à la défense sans avoir été soumis au juge.

46. Le Gouvernement admet que dans les affaires où, pour des motifs d'intérêt public, des éléments pertinents ou potentiellement pertinents n'ont pas été divulgués à la défense, il importe de veiller à l'existence de garanties suffisantes pour protéger les droits de l'accusé. Il considère que le droit anglais, en principe comme en pratique dans la cause du requérant, offrait le niveau requis de protection. [...]

48. Quant aux questions ayant trait à la loi de 1985 sur l'interception des communications, le Gouvernement fait observer que ce dispositif a été conçu pour garantir que l'interception des communications ne soit autorisée que lorsqu'elle est strictement nécessaire pour atteindre un but légitime et que la diffusion et la rétention de tous éléments interceptés soient limitées au minimum nécessaire pour atteindre le but ayant justifié l'autorisation d'intercepter. Ainsi, la loi cherchait tout à la fois à ménager un juste équilibre entre le droit de chaque individu au respect de sa vie privée, au sens de l'article 8 de la Convention, et la nécessité de recourir à des surveillances secrètes et de garantir que les mesures et méthodes appliquées en la matière restent confidentielles. En conséquence, il ne serait pas possible de conserver, divulguer et invoquer des éléments interceptés dans le cadre de procédures pénales, mais cette restriction s'appliquerait de manière identique à l'accusation et à la défense.

49. La Commission considère que la procédure pénale intentée à l'encontre du requérant a été équitable, étant donné que le juge de première instance, qui statua sur la question de la divulgation des preuves, connaissait tant le contenu des preuves non divulguées que la nature des arguments du requérant, et était ainsi à même de mettre en balance l'intérêt du requérant à une divulgation des éléments litigieux et l'intérêt public à leur dissimulation. Elle estime que la non-divulgation d'éléments ayant pu être interceptés n'a pas rendu la procédure inéquitable, dès lors que l'existence de pareils éléments n'a pas été établie, que le principe de l'égalité des armes a été respec-

té, puisqu'aucune des parties ne pouvait s'appuyer sur des preuves interceptées, et que le requérant aurait pu produire des preuves quant à la réalité et au contenu des appels téléphoniques qu'il disait avoir été passés, mais choisit de n'en rien faire.

50. La Cour rappelle que les exigences du paragraphe 3 de l'article 6 représentent des aspects particuliers du droit à un procès équitable garanti par le paragraphe 1 (arrêt Edwards c. Royaume Uni du 16 décembre 1992, série A n° 247-B, § 33). Eu égard aux circonstances de l'espèce, elle juge superflu d'examiner séparément sous l'angle du paragraphe 3 b) et d) les allégations du requérant, celles-ci s'analysant en un grief selon lequel l'intéressé n'a pas bénéficié d'un procès équitable. Aussi se bornera-t-elle à examiner la question de savoir si, considérée dans son ensemble, la procédure a revêtu un caractère équitable.

51. Tout procès pénal, y compris ses aspects procéduraux, doit revêtir un caractère contradictoire et garantir l'égalité des armes entre l'accusation et la défense : c'est là un des aspects fondamentaux du droit à un procès équitable. Le droit à un procès pénal contradictoire implique, pour l'accusation comme pour la défense, la faculté de prendre connaissance des observations ou éléments de preuve produits par l'autre partie (arrêt Brandstetter c. Autriche du 28 août 1991, série A n° 211, §§ 66-67). De surcroît, l'article 6 § 1 exige, comme du reste le droit anglais, que les autorités de poursuite communiquent à la défense toutes les preuves pertinentes en leur possession, à charge comme à décharge.

52. Toutefois, le requérant l'admet d'ailleurs, le droit à une divulgation des preuves pertinentes n'est pas absolu. Dans une procédure pénale donnée, il peut y avoir des intérêts concurrents – tels que la sécurité nationale ou la nécessité de protéger des témoins risquant des représailles ou de garder secrètes des méthodes policières de recherche des infractions – qui doivent être mises en balance avec les droits de l'accusé (voir, par exemple, l'arrêt Doorson c. Pays Bas du 26 mars 1996, *Recueil des arrêts et décisions* 1996-II, § 70). Dans certains cas, il peut être nécessaire de dissimuler certaines preuves à la défense, de façon à préserver les droits fondamentaux d'un autre individu ou à sauvegarder un intérêt public important. Toutefois, seules sont légitimes au regard de l'article 6 § 1 les mesures restreignant les droits de la défense qui sont absolument nécessaires (arrêt Van Mechelen et autres c. Pays Bas du 23 avril 1997, *Recueil* 1997-III, § 58). De surcroît, si l'on veut garantir un procès équitable à l'accusé, toutes difficultés causées à la défense par une limitation de ses droits doivent être suffisamment compensées par la procédure suivie devant les autorités judiciaires (arrêts Doorson précités, § 72, et Van Mechelen et autres précité, § 54).

53. Lorsque des preuves ont été dissimulées à la défense au nom de l'intérêt public, il n'appartient pas à la Cour de dire si pareille attitude était absolument nécessaire car, en principe, c'est aux juridictions internes qu'il revient d'apprécier les preuves produites devant elles. De toute manière, dans beaucoup d'affaires où, comme en l'occurrence, les preuves en question n'ont ja-

mais été révélées, il ne serait pas possible à la Cour de chercher à mettre en balance l'intérêt public à une non-divulgation des éléments litigieux et l'intérêt de l'accusé à se les voir communiquer. Aussi la Cour doit-elle examiner si le processus décisionnel a satisfait dans toute la mesure du possible aux exigences du contradictoire et de l'égalité des armes et s'il était assorti de garanties aptes à protéger les intérêts de l'accusé.

54. Le 14 janvier 1994, peu avant que ne s'ouvre le procès du requérant, l'accusation saisit le juge d'une requête unilatérale tendant à voir reconnaître une immunité d'intérêt public la dispensant de communiquer certains éléments en sa possession. La défense fut avisée qu'une requête allait être introduite mais ne fut pas informée de la catégorie dont relevaient les éléments que l'accusation souhaitait ne pas devoir divulguer. Elle se vit donner l'occasion d'exposer au juge les grandes lignes de son argumentation, qui consistait à dire que le requérant avait pris livraison de la cargaison de viande conformément à des instructions reçues par téléphone la nuit précédente et qu'il ignorait que la viande contenait du cannabis, et elle invita le juge à ordonner la divulgation de toutes preuves se rapportant à ces faits allégués. Le juge examina les éléments en question et décida qu'ils ne devaient pas être divulgués. La défense ne fut pas informée des motifs étayant cette décision.

55. La Cour considère que la défense a été tenue informée et a eu l'occasion de formuler des observations et de participer au processus décisionnel autant qu'il était possible sans que lui fussent divulgués les éléments de preuve que, pour des motifs d'intérêt public, l'accusation souhaitait ne pas devoir communiquer. S'il est vrai que, dans un certain nombre de contextes différents, le Royaume Uni a introduit ou est en train d'introduire un système prévoyant l'intervention d'un « avocat spécial », la Cour considère que pareille procédure n'était pas nécessaire en l'espèce. Elle relève en particulier que l'accusation ne s'est en l'occurrence nullement prévalu des éléments non divulgués, lesquels n'ont au demeurant jamais été portés à la connaissance du jury. Cette situation doit être distinguée de celles auxquelles les lois de 1997 [1] et 1998 [2] entendaient porter remède, à savoir celles où les décisions attaquées se fondaient sur des éléments aux mains de l'exécutif qui n'avaient jamais été soumis aux juridictions de contrôle.

56. Le fait que la nécessité d'une divulgation fut à tout moment sujette à l'appréciation du juge fournit une garantie supplémentaire importante, dès lors que le magistrat avait l'obligation de vérifier tout au long du procès que la non-divulgation des preuves n'était pas contraire à l'équité. Nul n'a prétendu que le juge n'était pas indépendant et impartial, au sens de l'article 6 § 1. Il avait une parfaite connaissance de l'ensemble des preuves et questions soulevées par l'espèce et, tant avant que pendant le procès, il s'est trouvé en

1) Ndr : loi sur la commission spéciale de recours en matière d'immigration (*Special Immigration Appeals Commission Act*)
2) Ndr : loi sur l'Irlande du Nord (*Northern Ireland Act*)

mesure de contrôler la pertinence pour la défense des informations non communiquées à celle-ci. On peut de plus supposer – notamment parce que la Cour d'appel confirma que le compte rendu de l'audience non contradictoire montrait que le juge avait « examiné de manière très attentive si les éléments litigieux étaient pertinents ou pouvaient l'être pour l'argumentation qui lui avait été exposée » – que le magistrat a appliqué les principes qui avaient peu auparavant été dégagés par la Cour d'appel et qui voulaient, par exemple, que dans la mise en balance de l'intérêt public à dissimuler des preuves, d'une part, et de l'intérêt de l'accusé à se les voir communiquer, de l'autre, un grand poids fût attaché à l'intérêt de la justice, et que le juge continuât à apprécier la nécessité d'une divulgation tout au long du procès. La jurisprudence de la Cour d'appel anglaise montre que l'appréciation à laquelle le juge doit se livrer remplit les conditions qui, d'après la jurisprudence de la Cour européenne, sont essentielles pour garantir un procès équitable dans les cas de non-divulgation d'éléments détenus par l'accusation. En l'occurrence, la juridiction interne de première instance a donc appliqué des normes qui respectaient les principes pertinents d'équité procédurale consacrés par l'article 6 § 1 de la Convention. De surcroît, une fois saisie, la Cour d'appel rechercha également si les preuves litigieuses auraient ou non dû être divulguées, offrant ainsi un degré accru de protection des droits du requérant.

57. Par ailleurs, M. Jasper allègue que son procès a aussi manqué d'équité en ce que le produit d'une interception téléphonique a été dissimulé à la défense sans avoir été soumis au juge. La Cour note toutefois qu'il n'est pas établi que pareil élément existât à l'époque du procès. De plus, dès lors qu'au titre de l'article 9 de la loi de 1985 il était interdit tant à l'accusation qu'à la défense de produire des preuves pouvant suggérer que des appels avaient été interceptés par des autorités de l'État, le principe de l'égalité des armes a été respecté. Au surplus, le requérant aurait pu témoigner lui-même ou faire témoigner d'autres personnes quant à la réalité et au contenu des instructions qu'il disait avoir reçues par téléphone le jour avant son arrestation.

58. En conclusion, la Cour estime que le processus décisionnel a satisfait autant que possible aux exigences du contradictoire et de l'égalité des armes et qu'il était assorti de garanties aptes à protéger les intérêts de l'accusé. Il s'ensuit qu'il n'y a pas eu violation de l'article 6 § 1 en l'espèce.

PAR CES MOTIFS, LA COUR,

1. Dit, par neuf voix contre huit, qu'il n'y a pas eu violation de l'article 6 § 1 de la Convention.

Chapitre V

Nouvelles brèves

Février

Europe

La Commission des libertés et des droits des citoyens a organisé les 22 et 23 février 2000 une audition publique sur le thème de « l'Union européenne et la protection des données ». Le journaliste Duncan CAMPBELL a décrit le système d'espionnage électronique connu sous le nom « d'Échelon ». Plusieurs firmes comme Thomson CSF ou Airbus Industries en auraient été victimes. La présidente de l'Europarlement souhaite que soit examinée d'urgence l'éventuelle responsabilité d'Etats membres de l'U.E. et des États-Unis et les moyens pour contrer le développement de ce type d'espionnage.

États-Unis d'Amérique

Des documents « top-secret » déclassifiés par l'agence américaine pour la sécurité nationale (NSA) confirment l'existence du programme Échelon.

Le réseau Échelon a été mis en place en 1948 par les États-Unis avec le concours de la Grande-Bretagne, du Canada, de la Nouvelle-Zélande et de l'Australie pour, au départ, recueillir des informations sur la situation militaire des éventuels adversaires de ces pays.

France

Le président de la commission de la défense à l'Assemblée nationale annonce la création, décidée à l'unanimité, d'une mission d'information parlementaire sur le réseau d'interception des télécommunications Échelon. Le rapporteur est le député UDF du Var, Arthur PAECHT. Un groupe de travail dans lequel chaque groupe politique sera représenté, sera associé à son activité.

Mars

France

Michelle AZZARO a été condamnée à 4 mois d'emprisonnement avec sursis et 100 000 francs d'amende pour avoir fait poser des micros dans les plinthes des bureaux de certains de ses salariés. Stéphane GRIGGIO, qui avait posé les micros, a été condamné à 20 000 francs d'amende pour complicité.

France

La DGSE est mise en cause par la presse spécialisée pour collaborer avec la NSA dans le domaine des interceptions de communications. L'agence américaine lui aurait transmis une partie de son savoir-faire dans les années 1970, facilitant ainsi la construction d'une quinzaine de stations d'écoutes en métropole ou en outre-mer, et des réunions régulières prolongeraient encore cette coopération. Un des résultats marquant serait la mise au point des logiciels d'analyse des correspondances interceptées.

Chine

Une association américaine affirme que le gouvernement chinois a renforcé en 1999 ses écoutes sur le réseau internet. Elle ajoute que ces interceptions serviraient parfois pour poursuivre des dissidents ou des journalistes.

France

Une plainte contre X du chef de violation du secret des correspondances a été déposée à Paris par une association de défense des utilisateurs d'internet. Elle vise en fait le réseau Échelon. La volonté des responsables de cette association est de « s'opposer systématiquement au contrôle des réseaux quand il y a atteinte grave aux libertés individuelles ».

Allemagne

La presse allemande affirme que la station d'écoute électronique américaine située à Bad Aibling en Bavière se consacrait notamment à l'espionnage d'entreprises allemandes. Elle aurait cessé sous la pression des autorités fédérales et viserait la Suisse. La station de Bad Aibling serait la plus importante base d'écoute américaine après celle de Menwith Hill en Grande-Bretagne.

Avril

Allemagne

La presse allemande indique que l'ancien Chancelier fédéral Helmut KOHL était surveillé et mis sur écoute par la STASI (police politique de l'ex-RDA) depuis l'âge de 20 ans. Ce service aurait été informé dès les années soixante de l'existence d'une caisse noire à la CDU. Certains enregistrements mettraient directement l'ancien Chancelier en cause. Celui-ci a annoncé qu'il s'opposerait à la publication des rapports d'écoutes non par craintes personnelles mais par principe. L'Office chargé d'exploiter les archives de la STASI posséderait de nombreuses écoutes de personnalités.

France

Durant le week-end pascal le vol d'un coffre-fort a été commis au siège de France Telecom Mobiles à Montrouge dans les Hauts-de-Seine. Ce coffre contenait de nombreux « cartons » d'écoutes administratives couvertes par le secret-défense. Quelques jours plus tard un vol avec effraction a été de nouveau tenté. La D.S.T. a été chargée de l'enquête. Les premiers éléments ont fait apparaître que les systèmes de sécurité ou de contrôle d'accès étaient inactivés.

Mai

Russie

Le groupe de presse Media-Most qui a fait l'objet d'une perquisition diligentée par le FSB (ex-KGB) a reconnu avoir utilisé dans ses locaux des écoutes téléphoniques et des détecteurs de mensonge pour garder la trace de certaines demandes extérieures. Les responsables du groupe ont déclaré avoir agi en toute légalité en l'absence de toute interdiction par la législation russe. Ils ont de plus démenti avoir enregistré les conversations de leurs journalistes avec des hauts responsables russes. De leur côté, les télévisions publiques ont affirmé que 2 500 dossiers de personnes intéressant le service de sécurité du groupe de presse avaient été saisis.

Russie

La police de Saint-Pétersbourg a arrêté un informaticien qui avait mis au point et vendait un système d'écoutes téléphoniques. Ce système composé d'un modem et d'un logiciel permettait, d'après la télévision locale, de réaliser des écoutes non seulement en Russie mais aussi à l'étranger. Son prix de vente : 5 000 $.

Juin

États-Unis d'Amérique

Le quotidien USA Today citant un responsable du FBI a annoncé que les autorités américaines avaient ordonné en 1999 un nombre jamais atteint d'écoutes téléphoniques pour des affaires de terrorisme ou d'espionnage. Celles-ci s'élevant à 484 en 1992 avaient connu une augmentation constante sous la présidence de Bill CLINTON pour atteindre le nombre de 880 l'année dernière.

États-Unis d'Amérique

La diffusion de comptes rendus d'interceptions de la NSA classés « secret » et relatifs notamment aux conversations d'Hilary CLINTON ainsi qu'à celles de l'ancien président Jimmy CARTER ont suscité un vif émoi chez les membres de la commission pour les affaires de renseignements de la Chambre des Représentants. Ces documents ont pu être obtenus après une procédure judiciaire intentée par une organisation non-gouvernementale et fondée sur le « Freedom of information Act ».

Salvador

La presse révèle que France-Telecom (actionnaire majoritaire de l'opérateur local) a été condamné par l'autorité de contrôle des télécommunications (Superintendencia de Electricidad y Telecomunicaciones, SET) à la plus forte amende prévue pour avoir procédé à des écoutes téléphoniques illégales au profit du service de renseignement de l'État (Organismo de Intelligencia del Estado). Les personnes écoutées étaient de simples particuliers, le procureur de la République, des hommes politiques, des journalistes, des associations ou des banques. L'entreprise a toujours nié les faits.

Juillet

Russie

Depuis le 5 juillet, il est possible de consulter sur le site de l'agence de journalisme d'investigation russe « Freelance Bureau » les dossiers de 140 personnalités. Ces dossiers constitués de transcriptions d'écoutes téléphoniques, de rapports de surveillance et notes diverses proviennent de différentes officines de détectives ou de services de sécurité d'entreprises privées.

Europe

Le Parlement européen met en place une commission temporaire d'enquête de 36 membres sur « Échelon » à la suite des rapports du journaliste écossais Duncan Campbell de 1998 et 1999, et de son audition publique devant la commission des libertés et des droits des citoyens de la justice et des affaires intérieures, ainsi que des documents publiés en début d'année 2000 confirmant l'existence de ce réseau.

France

Le parquet de Paris décide de l'ouverture d'une enquête préliminaire sur les interceptions de communications opérées par le réseau Échelon. Elle est confiée à la direction de la surveillance du territoire (D.S.T.).

Brésil

La presse publie les transcriptions de 400 heures d'écoutes téléphoniques et met ainsi au jour un système de corruption dans lequel apparaissent des personnels du gouvernement, un juge, un sénateur et des députés.

Royaume-uni

Le « Regulation of Investigatory Powers Act 2000 » a été adopté par le parlement britannique le 26 juillet. Cette loi actualise les pouvoirs des services de sécurité publics en matière d'interception de communications et leur permet désormais d'accéder au courrier électronique chez les fournisseurs d'accès et de services de l'internet.

États-unis

La presse se fait l'écho d'associations de protection des libertés individuelles qui dénonce le logiciel « Carnivore » du FBI. Ce logiciel permet l'analyse

du flot des données circulant sur l'internet et de séparer les « paquets » faisant partie d'un courrier électronique de ceux du web ; un tri par mots-clés étant ensuite possible.

Août

Bulgarie

Après la découverte de micros dans l'appartement du procureur général de la Bulgarie, le parlement a voté la mise en place d'une commission d'enquête chargée d'analyser la pratique du recours aux écoutes et d'examiner la législation afin de garantir les droits constitutionnels des citoyens.

Israël

Dans un rapport présenté à la commission des lois de la Knesset, le chef du service des écoutes de la police, a indiqué qu'il avait été procédé en 1999 à 1 756 interceptions de communications. Celles-ci sont soumises à l'accord d'un tribunal. Le Shin Beth, service de sécurité intérieur, peut également avec un aval judiciaire procéder à des écoutes qui dans ce cas, restent confidentielles.

Septembre

Russie

La nouvelle loi russe sur les interceptions de communications a été invalidée par la Cour suprême. La cour a estimé que les dispositions relatives à l'information des sociétés de communication étaient insuffisantes.

Octobre

Allemagne

La député écologiste Ilka Schröder a porté plainte contre X pour « exploitation et tolérance du système d'espionnage Échelon ». Elle a saisi le procureur général fédéral ainsi que le procureur compétent pour la ville de Bad Aibling où est installée une base américaine du réseau Échelon.

France

Le rapport d'information de la commission de la défense de l'Assemblée nationale sur le réseau Échelon toute en constatant la réalité de son existence estime que les performances d'Échelon « ont atteint leurs limites » notamment « parce que les moyens engagés ne sont plus en rapport avec l'explosion des communications dans le monde ». Il constate également que « si les preuves manquent pour évoquer l'espionnage industriel, les propos d'anciens responsables d'agences de renseignements constituent autant d'aveux ». Il propose pour se prémunir contre un danger potentiel pour les libertés publiques et individuelles entre autres la libéralisation des programmes de cryptographie ou de chiffrement, l'élaboration d'une véritable déon-

tologie du renseignement, l'engagement enfin de négociations internationales.

États-Unis

Le pentagone a décidé de reprendre à son profit l'exploitation du réseau de téléphonie d'Iridium.

Ce réseau de soixante-dix satellites avait été mis en faillite en début d'année.

Novembre

Belgique

Le comité de contrôle permanent des services de renseignements consacre une étude approfondie à l'existence et à l'activité du réseau « Échelon » dans son rapport complémentaire d'activité 1999 et publie notamment le rapport rédigé par les experts qu'il avait désignés en février 2000. Cette enquête avait été ouverte sur l'initiative du Parlement fédéral.

Bulgarie

Un membre du parquet de Sofia a affirmé que des dirigeants du parti de la minorité turque ainsi que le rédacteur en chef du plus grand journal bulgare étaient mis sur écoute.

Le ministre de l'intérieur a démenti ces affirmations.

Chine

Les autorités réglementent l'usage de l'internet. Les forums doivent effectuer une identification préalable de leurs participants et tout message illégal – c'est-à-dire par exemple portant atteinte à la sécurité nationale ou causant un tort à l'honneur et aux intérêts de la Chine ou encore propageant des superstitions féodales – doit être censuré et communiqué aux autorités avec l'identification de l'émetteur.

Liban

Le président du parlement a affirmé devant des députés que le Président de la République, les ministres, les parlementaires, les diplomates et les journalistes faisaient l'objet d'écoutes téléphoniques illégales. Cela résulterait notamment de l'absence des textes réglementaires d'application de la loi sur les écoutes adoptée fin 1998.

Décembre

France

Après l'Allemagne, l'Autriche et la Suisse en octobre, le Royaume Uni au début du mois, les « Big brothers awards » ont été décernés en France à l'initiative d'associations de protection des citoyens par un jury composé de militants associatifs, journalistes, avocats, universitaires et autres intellectuels, à cent hommes ou institutions, qui mettent le plus en péril les libertés individuelles.

Cuba

Lors d'une visite des installations avec Fidel CASTRO, le président russe, Vladimir POUTINE, a déclaré dans une conférence de presse, que son pays et Cuba étaient intéressés par le maintien de l'activité de la base d'écoutes électronique de Lourdes, dans la banlieue de la Havane.

Environ 1500 personnes travailleraient dans ce centre doté de matériels de Haute technologie et dont les États – Unis exigent le démantèlement.

France

Le Conseil constitutionnel déclare contraire à la Constitution la disposition législative faisant supporter aux opérateurs les investissements réalisés pour les interceptions de communications ainsi qu'une partie des coûts d'exploitation.

Europe

Le Conseil de l'Europe a rendu publique en octobre la 22e version de son projet de convention sur la cyber-criminalité. Ce texte qui vise à harmoniser les législations nationales non seulement des États membres mais également de tous autres États intéressés dont les États-Unis organise notamment les perquisitions et saisies de données informatiques, la collecte et la conservation de données de trafic ou stockées ainsi que l'interception de communications électroniques.

Différentes associations à travers le monde ont dénoncé le risque que ce traité constitue pour la vie privée.

En fin d'année, les experts européens rédigeaient la 25e version de ce texte.

Bibliographie

Claudine Guerrier, *Les écoutes téléphoniques*, CNRS Droit, CNRS éditions, 2000

Arthur Paecht, *Échelon : mythe ou réalité ?*, 2000, nº 2623 Rapport d'information déposé par la Commission de la défense nationale et des forces armées sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale.

Arthur Paecht, *Rapport parlementaire n° 1951* fait au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi Nº 1497 du M. Paul QUILES et autres, tendant à la création d'une délégation parlementaire pour les affaires de renseignements, enregistré à la présidence de l'Assemblée nationale le 23 novembre 1999.

Virginie Peltier, *Le secret des correspondances*, Presse universitaire d'Aix Marseille, faculté de droit et de science politique, 1999.

François Thuilier, *L'Europe du secret : Mythes et réalité du renseignement politique interne*, La Documentation française, 2000.

Bertrand Warusfel, *Contre-espionnage et protection du secret : histoire, droit et organisation de la sécurité nationale en France*, édition Lavauzelle, 2000.

Index

E

F

G

I

J

L

M

N

O

P

Q

R

S

T

U

V

Table des matières