

# Sommaire

|                                                                          |    |
|--------------------------------------------------------------------------|----|
| <b>Avant-propos</b> .....                                                | 5  |
| <br>Première partie                                                      |    |
| <b>RAPPORT D'ACTIVITÉ</b> .....                                          | 7  |
| <br>Chapitre I                                                           |    |
| <b>Organisation et fonctionnement de la Commission</b> .....             | 9  |
| <br>Chapitre II                                                          |    |
| <b>Le contrôle des autorisations</b> .....                               | 13 |
| <br>Chapitre III                                                         |    |
| <b>Le contrôle de l'exécution</b> .....                                  | 25 |
| <br>Chapitre IV                                                          |    |
| <b>Le contrôle du matériel</b> .....                                     | 29 |
| <br>Chapitre V                                                           |    |
| <b>Actualités de l'année 2003</b> .....                                  | 33 |
| <br>Deuxième partie                                                      |    |
| <b>ÉTUDES ET DOCUMENTS</b> .....                                         | 35 |
| <br>Chapitre I                                                           |    |
| <b>Présentation ordonnée des textes relatifs aux interceptions</b> ..... | 37 |

|                                                                                 |    |
|---------------------------------------------------------------------------------|----|
| Chapitre II                                                                     |    |
| <b>Actualité législative</b> . . . . .                                          | 49 |
| Chapitre III                                                                    |    |
| <b>Réflexions sur le motif d'interception « sécurité nationale »</b> . . . . .  | 53 |
| Chapitre IV                                                                     |    |
| <b>Réflexions sur le motif d'interception « protection économique »</b> . . . . | 59 |
| Chapitre V                                                                      |    |
| <b>Interceptions de sécurité et secret défense</b> . . . . .                    | 63 |
| Chapitre VI                                                                     |    |
| <b>Jurisprudence</b> . . . . .                                                  | 65 |
| Chapitre VII                                                                    |    |
| <b>Questions parlementaires</b> . . . . .                                       | 75 |

## Avant-propos

*L'année 2003 a été placée, pour la Commission sous le signe du changement : changement dans les personnes, et changement dans les procédures.*

*La composition de la Commission a été renouvelée en la personne de son président et de monsieur Bernard DEROSIER, député du Nord. Le directeur du GIC, principal correspondant de la Commission, a également changé au cours de cette période, le général EPIS ayant succédé à l'amiral LE BAL'CH. Par ailleurs, un nouveau chargé de mission, Rémi RÉCIO, magistrat, a été nommé dans les services de la Commission.*

*Ce changement s'est toutefois effectué dans la continuité, la « jurisprudence » de la Commission étant maintenant bien établie après plus de dix ans d'application de la loi de 1991. Qu'il me soit permis à cette occasion de rendre hommage à l'action entreprise et développée par mon prédécesseur, le président MANDELKERN, soutenu par ses assesseurs parlementaires, au cours des six années de son mandat. Il a renforcé l'autorité et la crédibilité de la Commission vis-à-vis des services qui utilisent les interceptions. Il a progressivement mis au point des approches juridiques adaptées à l'évolution des techniques et des formes de criminalité.*

*C'est dans les derniers mois de sa présidence qu'est intervenu un changement majeur dans les procédures de contrôle. Je me réfère à l'acceptation par le Premier ministre, à la suggestion*

*de la Commission, de l'extension du contrôle a priori sur toutes les demandes, y compris les demandes présentées en urgence absolue. Cette nouvelle procédure, qui représente un progrès incontestable sur le plan des garanties données au citoyen, donne jusqu'à présent toute satisfaction.*

*Un point noir est en revanche apparu, qui sera commenté dans le corps du rapport. Il s'agit de l'augmentation très sensible du pourcentage des demandes initiales présentées selon la procédure d'urgence absolue. La proportion de ces demandes par rapport au total des demandes initiales a en effet augmenté de plus de 40 % par rapport à 2002. Sans méconnaître les impératifs de protection des personnes et des biens qui peuvent justifier pour certains types de menaces une augmentation conjoncturelle du recours à cette procédure, la Commission est sérieusement préoccupée par cette tendance. La procédure d'urgence absolue ne permet pas en effet une étude et un contrôle aussi approfondi que nécessaire des dossiers.*

*Ceci étant dit, le bilan de l'action de la Commission en 2003, menée en bonne coopération avec les services demandeurs, est globalement positif. Un instrument efficace a été mis au point avec l'appui technique du groupement interministériel de contrôle. J'entends poursuivre, avec la Commission et l'assistance de nos magistrats, l'action de mes prédécesseurs dans la recherche d'un équilibre toujours délicat entre la protection de la vie privée et les impératifs de la protection de l'ordre public et des intérêts supérieurs de l'État.*

Jean-Louis DEWOST  
*Président de la Commission*

Première partie

# RAPPORT D'ACTIVITÉ

# Organisation et fonctionnement de la Commission

## Composition de la Commission

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

Jean-Louis DEWOST, président de section au Conseil d'État nommé président pour une durée de six ans par le président de la République (décret du 29 septembre 2003, publié au *Journal officiel* le 30 septembre 2003). Jean-Louis DEWOST a succédé le 1<sup>er</sup> octobre 2003 à Dieudonné MANDELKERN,

André DULAIT, sénateur (UC) des Deux-Sèvres, désigné par le président du Sénat à la suite du renouvellement partiel du Sénat de 2001,

Bernard DEROSIER, député (PS) du Nord, désigné par le président de l'Assemblée nationale le 20 mars 2003.

La Commission est assistée de deux magistrats de l'ordre judiciaire : Gérard LORHO, délégué général depuis sa nomination en date du 17 décembre 2001,

Rémi RECIO, chargé de mission depuis le 19 décembre 2003.

Le secrétariat est assuré par Josiane MEURICE et Françoise NUDELMANN.

## Rappel des compositions successives de la Commission

- *Présidents*

Paul BOUCHET, conseiller d'État, 1<sup>er</sup> octobre 1991,  
Dieudonné MANDELKERN, président de section au Conseil d'État, 1<sup>er</sup>  
octobre 1997,  
Jean-Louis DEWOST, président de section au Conseil d'État, 1<sup>er</sup> octobre  
2003.

- *Représentants de l'Assemblée nationale*

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

- *Représentants du Sénat*

Marcel RUDLOFF, sénateur du Bas-Rhin, 17 juillet 1991,  
Jacques THYRAUD, sénateur du Loir-et-Cher, 26 mars 1992,  
Jacques GOLLIET, sénateur de Haute-Savoie, 22 octobre 1992,  
Jean-Paul AMOUDRY, sénateur de Haute-Savoie, 14 octobre 1995,  
Pierre FAUCHON, sénateur du Loir-et-Cher, 18 septembre 1998,  
André DULAIT, sénateur des Deux-Sèvres, 6 novembre 2001.

- *Agents de la Commission*

- Délégués généraux

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

- Chargés de mission

Jean-Hugues GAY, magistrat, 6 septembre 1996,  
Laurent BECUYWE, magistrat, 3 mai 1999,  
Rémi RECIO, magistrat, 19 décembre 2003.

- Secrétariat administratif

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

– Secrétariat comptable

Josiane MEURICE, 21 avril 1995.

– Chauffeur

Jean-François LAMBELET, 1<sup>er</sup> janvier 1999

## 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 2003, les crédits votés représentent 363 179 euros dont 267 695 au titre des frais de personnel et 95 484 au titre des frais de fonctionnement. En outre, la Commission a bénéficié sur son budget 2003 d'un report de crédits de 9 000 euros au titre des rémunérations, frais de personnel et prestations sociales.

## Fonctionnement

Conformément à l'article 1<sup>er</sup> 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 n° 97-757 du 10 juillet 1997 qui, sous la présidence du secrétaire général de la Défense nationale, émet des avis sur les demandes de commercialisation ou d'acquisition des matériels susceptibles de porter atteinte au secret des correspondances.

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

# Le contrôle des autorisations

## Les modalités du contrôle

### Déroulement du contrôle

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

La pratique du contrôle préalable à la décision d'autorisation, contrairement à la lettre de l'article 14 de la loi du 10 juillet 1991, permet de nouer un dialogue utile avec les services demandeurs et une meilleure prise en compte par ceux-ci, en amont, des éléments de la « jurisprudence » de la Commission grâce au relais centralisé que constitue le groupement interministériel de contrôle (GIC).

Enfin le président de la Commission est informé par le GIC des décisions prises par le Premier ministre ou les personnes déléguées par celui-ci dans les conditions prévues par la loi de 1991. En cas de désaccord, hypothèse non rencontrée depuis 1997, il soumet la divergence d'appréciation à la délibération de la Commission conformément à l'article 14 de la loi. Dans l'hypothèse où le désaccord est confirmé, une recommandation tendant à l'interruption de l'interception en cause est adressée au Premier ministre.

### Contrôle formel et respect des contingents

L'activité de contrôle comporte en premier lieu un aspect formel qui consiste à vérifier que les signataires des demandes d'autorisation ont bien

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

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

Cette vérification fait ressortir en 2003 des encours moyens mensuels allant de 1200 à 1400 avec une moyenne annuelle de 1350 contre 1 207 en 2002 et 1 108 en 2001.

Rappelons que l'extension massive du parc téléphonique imputable au GSM, notamment aux cartes prépayées, et l'impulsion donnée à la lutte contre la criminalité et la délinquance organisées, notamment par la création des GIR (groupements d'intervention régionaux), se sont traduites fin 2002 par une augmentation des contingents d'interceptions au profit du ministère de la Défense (gendarmerie) et du ministère chargé des Douanes.

S'agissant du ministère de la Défense, la demande était justifiée par les besoins de la Gendarmerie nationale. Pour ce qui concerne le ministère des Finances, le quota de 20 lignes, inchangé depuis 1991, n'apparaissait plus réaliste au regard de l'accroissement rapide des contrebandes diverses et des flux financiers suspects, les deux phénomènes relevant des compétences respectives de la direction générale des douanes et droits indirects (DGDDI) et du service de traitement du renseignement et action contre les circuits financiers clandestins (TRACFIN). Consultée par le Premier ministre, la Commission (CNCIS, 11<sup>e</sup> rapport 2002, p. 37) a émis un avis favorable aux augmentations souhaitées qui ont reçu application depuis le 1<sup>er</sup> janvier 2003. Le tableau ci-dessous résume l'évolution des contingents d'interception depuis la création de la CNCIS. La Commission avait en son temps souligné la faiblesse du contingent accordé aux Douanes et était favorable à un relèvement du plafond.

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

Tableau récapitulatif

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

*N.B.* : antérieurement à la loi de 1991, les informations disponibles ne sont pas complètes.

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

Le système par lequel les interceptions sont contingentées – leur nombre ne peut à aucun moment dépasser un plafond fixé par ministère en vertu d'une décision du Premier ministre, la répartition entre les services étant du ressort de chaque ministère – conduit à ce que le nombre moyen annuel des interceptions est systématiquement inférieur au contingent : les services doivent en effet se réserver la possibilité de répondre en permanence à des circonstances inattendues ou à des besoins nouveaux.

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

### **Justification de la demande d'interception de sécurité**

Comme leur nom l'indique, le premier et le seul objectif des interceptions de sécurité est la protection des intérêts fondamentaux de la nation. Les motifs prévus par la loi du 10 juillet 1991 ne font que décliner les différents aspects de la sécurité, mais la référence précise à ceux-ci permet une première appréciation des demandes. On rappellera ici que ces motifs, énumérés à l'article 3 de la loi, sont : la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées. Les services demandeurs doivent faire référence explicite à l'un de ces motifs. Ils doivent en outre justifier leur demande par des explications circonstanciées qui permettront à la Commission d'apprécier l'articulation du fait au droit.

Le président de la CNCIS peut demander les éléments d'informations complémentaires qui lui sont nécessaires pour fonder son avis. Il formule

également les observations qu'il juge utiles sur la pertinence du motif invoqué. Il s'assure que la demande respecte le principe de proportionnalité entre le but recherché et la mesure sollicitée : la gravité du risque ou du danger pour la sécurité des personnes, qu'elles soient physiques ou morales, ou pour la sécurité collective, doit être à la mesure de l'atteinte à la vie privée que constitue la surveillance de la correspondance par la voie des télécommunications, et justifier cette atteinte. La recherche de cette proportionnalité peut aussi se traduire par une restriction au cas par cas de la durée maximale légale de la mesure qui est de quatre mois, par l'instruction donnée d'exclure certaines parties des conversations des transcriptions (appelées « productions ») et par une demande aux services d'établir un bilan circonstancié avant aval d'une nouvelle prolongation d'une interception plusieurs fois renouvelée. Il faut enfin que le but recherché ne puisse être rempli aussi bien par d'autres moyens.

### **Exigence de sécurité et protection des libertés**

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

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

La « jurisprudence » de la CNCIS s'attache également à la protection des libertés de conscience et d'expression. Ainsi maintient-elle que le prosélytisme religieux, comme l'expression d'idéologies extrêmes, ne justifient pas en tant que tels une demande d'interception s'ils ne comportent aucune menace pour l'ordre public, matérialisée par exemple par un appel à la violence.

D'une manière générale et quel que soit le motif, l'implication de la cible dans des agissements attentatoires à notre sécurité doit être au moins présumée (*cf.* développements *infra* page 58).

## **Données chiffrées et commentaires**

### **Demandes initiales**

Avec un contingent en hausse de 130 lignes, les demandes initiales, avec un total de 3362 demandes contre 3138 en 2002 ont enregistré une hausse de 7 %.

## Renouvellements

Les renouvellements ont enregistré une hausse du même ordre passant de 1572 en 2002 à 1677. La présentation de l'argumentation des demandes structurée par certains services sous la forme de trois paragraphes aux intitulés suivants : objectifs initiaux, résultats obtenus, résultats attendus, est particulièrement heureuse. Elle devra être généralisée courant 2004.

## Urgences absolues

Sur un total de 3362 demandes initiales, 548 (contre 363 en 2002), ont été acheminées selon la procédure dite d'urgence absolue représentant 16,3 % du total des demandes, soit près de 5 points de plus que l'an passé.

Cette augmentation est impressionnante. Elle devra être contenue à l'avenir sauf à vider de son sens le caractère exceptionnel que doit revêtir la procédure d'urgence absolue (si tout est urgent, rien ne l'est...).

Certes cette augmentation doit, pour une part, être relativisée par la part croissante des urgences absolues dites « techniques » destinées à prévenir l'interruption d'une surveillance en raison d'un changement de portable ou de carte prépayée par la cible. Ces urgences techniques pratiquées depuis fin juin 2003 ont représenté, pour un total de 70 demandes, 13 % des demandes présentées en urgence absolue. Toutefois, même si l'on déduit ces 70 demandes et qu'on les ajoute aux demandes du circuit normal par lequel elles étaient jusque là présentées, l'augmentation des urgences absolues est encore de 2 points soit 14 %, ce qui est loin du taux de 8 % antérieur à 2001.

La part croissante des urgences absolues a eu dans un premier temps pour effet d'éroder la part du contrôle exercé *a priori* par la Commission.

Un rappel est à ce propos nécessaire. Aux termes de la loi du 10 juillet 1991 (art. 14) la Commission, si elle n'est pas d'accord avec la décision d'interception prise par le Premier ministre, adresse à celui-ci une recommandation tendant à ce que cette interception soit interrompue. La Commission est donc censée émettre un avis *a posteriori*. Mais, dès les premiers mois de fonctionnement de la Commission, il est apparu que la solution adoptée n'était pas satisfaisante (CNCIS, 10<sup>e</sup> rapport 2001, p. 62). En effet la recommandation de la Commission survenait alors que l'interception des communications était déjà réalisée. Par ailleurs, les services, soucieux de la continuation de l'interception produisaient parfois des informations complémentaires, qui, si elles avaient figuré dans la demande initiale par trop succincte, auraient pu conduire la Commission à ne pas prendre de recommandation.

Pour ces raisons, le Premier ministre accepta rapidement la proposition selon laquelle la Commission serait consultée *a priori*, pratique qui n'a jamais été remise en cause.

Une exception demeurerait toutefois en ce qui concernait les demandes d'interceptions présentées en urgence absolue. Dans ce cas la décision était prise par le Premier ministre. La Commission ne manquait d'ailleurs pas dans ses rapports successifs de dénoncer un recours excessif à cette procédure dans des cas où l'urgence n'apparaissait pas flagrante alors que ceci privait la Commission de son contrôle *a priori*.

Pour accélérer et améliorer son information, ceci dans le contexte de l'affaire Schuller-Maréchal, la Commission adopta une recommandation le 28 février 1995 tendant à une information immédiate de la Commission de l'autorisation accordée (CNCIS, 4<sup>e</sup> rapport 1995, pages 27 à 34).

Début 2003, suite à une nouvelle hausse des demandes en urgence absolue, traduisant sans doute une volonté de meilleure réactivité de la part des services, le Premier ministre accepta la proposition de la Commission tendant à généraliser son contrôle *a priori* sur toutes les demandes, urgentes ou non. Cette nouvelle procédure mise en place le 10 mars et qui constitue le fait majeur de l'année donne toute satisfaction. Depuis cette date, 420 demandes ont été traitées selon cette procédure et dans cinq cas seulement, ce qui atteste de la disponibilité d'une petite structure comme celle de la Commission, l'avis n'a pu être émis qu'*a posteriori*. La Commission a émis six avis défavorables et fait huit observations. De nombreuses réserves, non formalisées mais récurrentes, ont été faites sur la réalité de l'urgence alléguée traduisant davantage dans plusieurs cas la volonté pour certains services de raccourcir le délai de recueil des signatures utiles que la nécessité de parer à un danger imminent. Un indicateur pertinent de cette dérive peut être trouvé dans l'examen des demandes de renouvellements. La Commission s'est ainsi penchée pour chaque renouvellement sur l'origine des demandes initiales et la répartition entre procédure normale et procédure d'urgence. Il est apparu que, pour un service, 25 % des demandes de renouvellements prenaient leur source dans une demande en urgence absolue. Si l'analyse de l'imminence d'une menace est toujours chose difficile, il n'en demeure pas moins qu'une interception sollicitée en urgence, pour parer à un risque conjoncturel, n'a pas en principe vocation à être prolongée. Dans le cas cité plus haut, un tel taux de renouvellement conduit à l'évidence à s'interroger *a posteriori* sur la réalité de l'urgence alléguée initialement. C'est pourquoi il convient de rappeler que ces demandes urgentes mais presque toujours tardives privent la Commission des avantages de l'examen approfondi qu'offre le circuit normal validé hebdomadairement et prive par voie de conséquence, les pouvoirs publics des garanties de cet examen. Ces demandes, même si la Commission a fait en sorte de se rendre disponible pour les examiner *a priori* dans les proportions rappelées ci-dessus doivent donc rester exceptionnelles.

## Motifs

C'est à nouveau le motif criminalité et délinquance organisées qui demeure le premier motif avec 50 % des demandes initiales, en légère hausse par rapport à l'an passé. Il est suivi par la prévention du terrorisme (33 %), la sécurité nationale (16 %) et la sauvegarde du patrimoine scientifique et économique (1 %).

Il est intéressant de noter que la part du motif criminalité et délinquance organisées, qui occupait déjà la première place en 1996 avec 40 %, contre 37 % pour le motif terrorisme, a crû de 10 % en huit ans. Les étapes majeures de cette progression ont consisté dans l'augmentation du contingent du ministère de la Défense consentie en 1997 au profit de la Gendarmerie nationale et celle consentie fin 2002 pour satisfaire, une fois encore, les besoins de la Gendarmerie nationale et ceux des Douanes pour la lutte contre les trafics recrudescents.

Les proportions sont très sensiblement différentes s'agissant des renouvellements : la prévention du terrorisme occupe la première place avec 46 % suivie de la sécurité nationale (40 %) et de la criminalité et délinquance organisées (13 %).

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

Au total (demandes initiales et renouvellements), le terrorisme représente 38 % des demandes, suivi de la criminalité organisée, 37 % et de la sécurité nationale, 24 %. En se reportant aux premiers chiffres disponibles (CNCIS, 4<sup>e</sup> rapport 1995) on relève la part légèrement inférieure du terrorisme (40 %), celle identique de la sécurité nationale, (24 %), mais sensiblement plus faible de la criminalité organisée, (29,5 %). Ce dernier motif a donc progressivement mordu sur les autres motifs.

## Bilan des observations

385 demandes (initiales ou de renouvellements) ont donné lieu à des observations contre 303 en 2002.

Sur ces 385 observations, on relève 87 avis négatifs contre 104 en 2002. Ces avis négatifs se partagent en 45 pour les demandes initiales et 42 pour les renouvellements, tous suivis par le Premier ministre. Ce dernier a en outre rejeté d'office trois demandes et cinq autres ont été abandonnées par les services suite à des demandes de renseignements complémentaires exprimées par la Commission.

Au total, avec 4994 interceptions réalisées (3317 interceptions initiales et 1677 renouvellements) contre 4654 en 2001, force est de constater à nouveau, malgré l'augmentation notée en 2003, qu'au regard de l'évolution du parc téléphonique (41,7 millions de portables en fin 2003 et 33,9 de téléphones filaires), les interceptions de sécurité demeurent la mesure d'exception voulue par la loi. Ce caractère exceptionnel est encore accentué par le fait que la surveillance d'une personne peut requérir l'interception d'autant de vecteurs que celle-ci en possède (filaire, GSM, fax) et que chaque vecteur intercepté comptera pour une interception. Dès lors les 3317 interceptions initiales concernent moins de 3000 personnes.

À titre de comparaison, même si celle-ci n'est pas aisée, on a dénombré respectivement 12700 et 16200 interceptions judiciaires pour les années 2002 et 2003 (ces chiffres ne distinguant pas entre interceptions initiales et renouvellements).

Une réflexion est d'ailleurs en cours intéressant tant les interceptions de sécurité que les interceptions judiciaires sur la « juste rémunération » des opérateurs de télécommunications.

## Tableaux annexes

### Les demandes de construction

#### État des demandes initiales d'interceptions, années 2002 et 2003

|               | Demandes initiales |            | Dont urgence absolue |            | Accordées  |            |
|---------------|--------------------|------------|----------------------|------------|------------|------------|
|               | Année 2002         | Année 2003 | Année 2002           | Année 2003 | Année 2002 | Année 2003 |
| <b>Totaux</b> | 3 138              | 3 362      | 363                  | 548        | 3 082      | 3 317      |

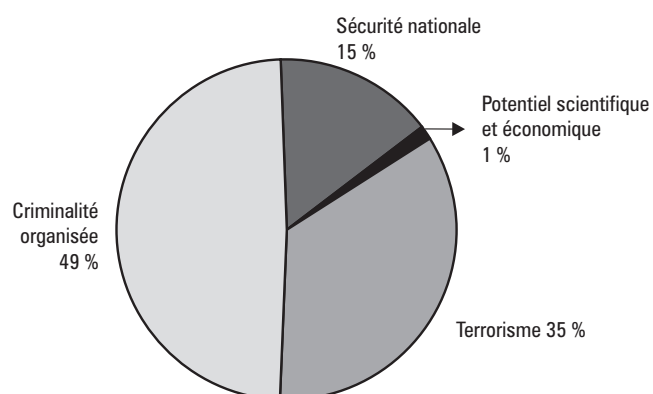
#### État comparatif sur cinq ans

| Motifs                               | 1999         | 2000         | 2001         | 2002         | 2003         |
|--------------------------------------|--------------|--------------|--------------|--------------|--------------|
| Sécurité nationale                   | 495          | 449          | 509          | 486          | 526          |
| Potentiel scientifique et économique | 87           | 72           | 49           | 38           | 42           |
| Terrorisme                           | 1 317        | 979          | 1 203        | 1 103        | 1 126        |
| Criminalité organisée                | 1 145        | 1 256        | 1 400        | 1 511        | 1 668        |
| Groupements dissous                  | 0            | 0            | 0            | 0            | 0            |
| <b>Totaux</b>                        | <b>3 044</b> | <b>2 756</b> | <b>3 161</b> | <b>3 138</b> | <b>3 362</b> |

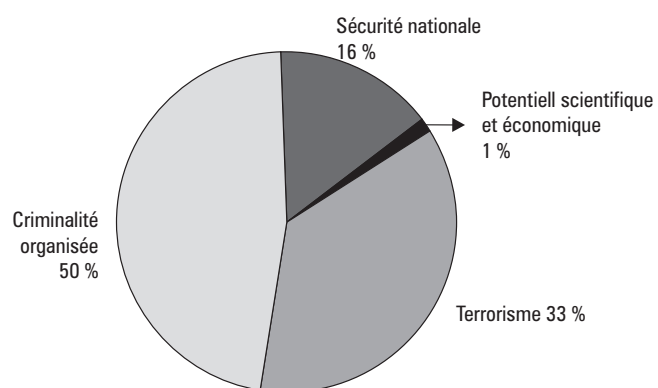
## Demandes initiales

### Répartition des motifs

2002



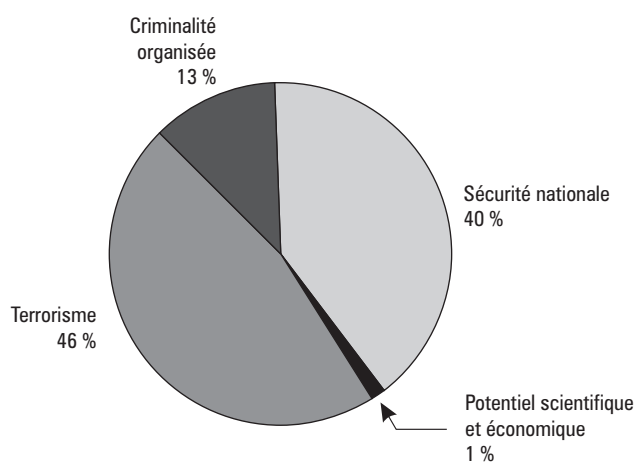
2003



## Les renouvellements d'interception

### Répartition des motifs (renouvellements accordés), année 2003

| Sécurité nationale | Potentiel scientifique et économique | Terrorisme | Criminalité organisée | Groupements dissous | Total |
|--------------------|--------------------------------------|------------|-----------------------|---------------------|-------|
| 663                | 22                                   | 782        | 210                   | 0                   | 1 677 |



### État comparatif sur cinq ans

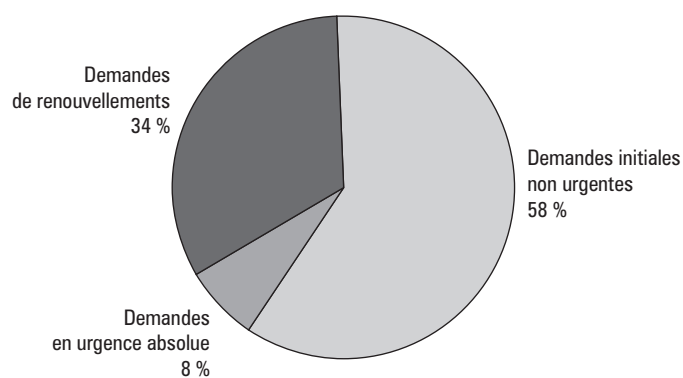
| Motifs                               | 1999         | 2000         | 2001         | 2002         | 2003         |
|--------------------------------------|--------------|--------------|--------------|--------------|--------------|
| Sécurité nationale                   | 597          | 551          | 559          | 539          | 663          |
| Potentiel scientifique et économique | 99           | 27           | 17           | 3            | 22           |
| Terrorisme                           | 719          | 744          | 667          | 814          | 782          |
| Criminalité organisée                | 181          | 163          | 174          | 216          | 210          |
| Groupements dissous                  | 3            | 1            | 0            | 0            | 0            |
| <b>Totaux</b>                        | <b>1 599</b> | <b>1 486</b> | <b>1 417</b> | <b>1 572</b> | <b>1 677</b> |

## Activité de la CNCIS : demandes initiales et renouvellements

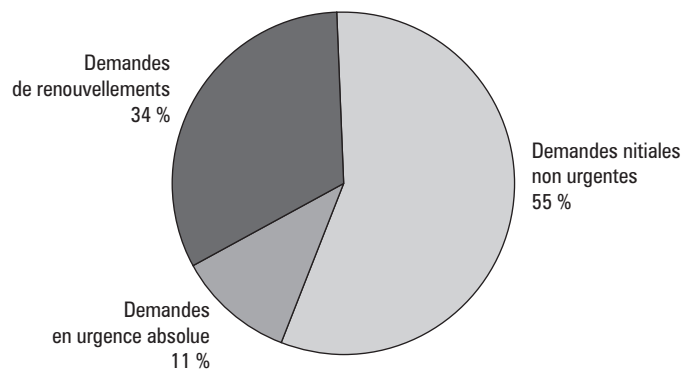
### Répartition des demandes entre interceptions et renouvellements d'interceptions

| Demandes initiales |            | Demandes initiales en urgence absolue |            | Demandes de renouvellements |            |
|--------------------|------------|---------------------------------------|------------|-----------------------------|------------|
| Année 2002         | Année 2003 | Année 2002                            | Année 2003 | Année 2002                  | Année 2003 |
| 2 775              | 2 814      | 363                                   | 548        | 1 629                       | 1 719      |

#### 2002

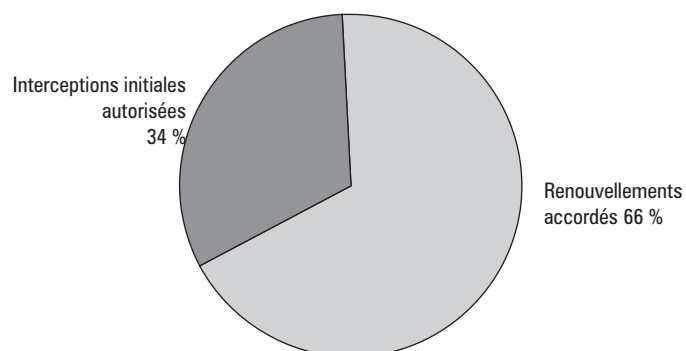


#### 2003

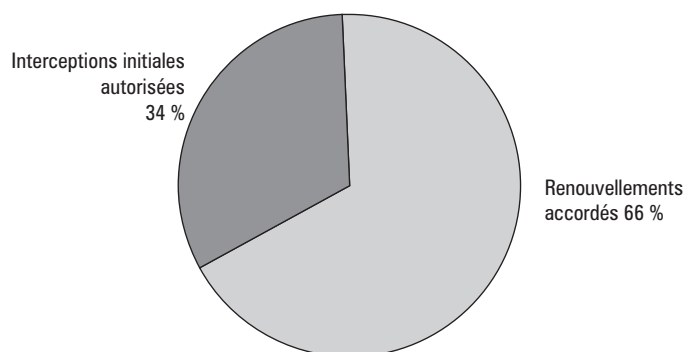


### Répartition entre autorisations d'interceptions et autorisations de renouvellements

**2002**



**2003**



### Demandes d'interceptions : tableau récapitulatif global sur cinq ans

| Type de demandes                   | 1999         | 2000         | 2001         | 2002         | 2003         |
|------------------------------------|--------------|--------------|--------------|--------------|--------------|
| Demandes initiales d'interceptions | 2 690        | 2 559        | 2 773        | 2 775        | 2 814        |
| Dont urgence absolue               | 354          | 197          | 388          | 363          | 548          |
| Demandes de renouvellements        | 1 643        | 1 533        | 1 464        | 1 629        | 1 677        |
| <b>Total</b>                       | <b>4 687</b> | <b>4 289</b> | <b>4 625</b> | <b>4 767</b> | <b>5 039</b> |

## Le contrôle de l'exécution

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

### Enregistrement, transcription et durée des interceptions

La mise en place en 2002 d'un effacement automatisé de l'enregistrement au plus tard à l'expiration du délai de dix jours, prévu par l'article 9 de la loi, s'est traduite par un gain de temps appréciable pour les agents chargés de l'exploitation. Le registre normalisé mis précédemment en place pour faciliter le contrôle a été revu pour tenir compte de cette évolution.

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

Quant aux transcriptions, elles doivent être détruites, conformément à l'article 12 de la loi du 10 juillet 1991, dès que leur conservation n'est plus indispensable à la réalisation des fins mentionnées à l'article 3. Depuis la mise en place, en 1996, du système centralisé de contrôle des destructions pour la région parisienne, il a été observé que les transcriptions conservées par les services au-delà de quatre mois étaient devenues résiduelles.

La durée des interceptions prévue par l'article 6 de la loi du 10 juillet 1991 est de quatre mois au plus. Une interception peut toutefois être prolongée pour quatre mois par renouvellement de l'autorisation avant l'expiration de la période en cours. La loi ne fixe pas de limite au nombre des renouvellements mais, comme il a été dit plus haut, ceux-ci font l'objet d'une grande attention de la part de la Commission.

## Le contrôle du GIC

Service du Premier ministre, consacré comme tel après trente et une années d'existence par le décret n° 2002-497 du 12 avril 2002 (CNCIS, 11<sup>er</sup> rapport 2002, p. 50), le GIC est l'élément clef du dispositif des interceptions de sécurité. Il en assure la centralisation conformément à l'art. 4 de la loi du 10 juillet 1991 (« le Premier ministre organise la centralisation de l'exécution des interceptions autorisées »).

Ce service est contraint de s'adapter constamment à la mesure des avancées technologiques incessantes dans le domaine des télécommunications qui constituent pour lui autant de défis à relever.

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

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

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

Les petits sites d'écoutes disséminés de façon empirique sur tout le territoire, souvent installés dans des conditions précaires, ont quasiment disparu. Le maillage du territoire en antennes principales et secondaires sécurisées, venant après la nécessaire étape de restructuration centralisée, atteste de la volonté de restituer aux services enquêteurs la proximité attendue.

## Les visites sur le terrain

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

d'interception, des installations et, comme en 2002, des opérateurs de télécommunication.

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

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

Au total, sous une forme ou sous une autre, six visites de services intéressant les régions Nord-Pas-de-Calais, Midi-Pyrénées, PACA, Centre, Bourgogne, Rhône-Alpes, ont été effectuées. À chaque fois les représentants de la CNCIS dressent un inventaire des pratiques et procédures mises en œuvre par les services pour l'application de la loi du 10 juillet 1991, apportent les informations et éclaircissements utiles, notamment sur le rôle de la CNCIS, recueillent les observations des personnels rencontrés et s'informent des réalités locales se rapportant aux motifs légaux des interceptions.

Les représentants de la CNCIS se sont rendus à nouveau (CNCIS, 11<sup>er</sup> apport 2002, p. 28) à la direction générale de la Gendarmerie nationale pour y visiter la section des interceptions de sécurité installée dans de nouveaux locaux, permettant de répondre à l'augmentation du contingent d'interceptions de 50 lignes qui a été accordé à la gendarmerie fin 2002.

## **Réclamations de particuliers et dénonciation à l'autorité judiciaire**

### **Les saisines de la CNCIS par les particuliers**

Cette année, trente-deux particuliers ont saisi par écrit la CNCIS. Une minorité des courriers concernait des demandes de renseignements sur la législation. La majorité, constituée de réclamations, a donné lieu au contrôle systématique auquel il est procédé lorsque le demandeur justifie d'un intérêt direct et personnel à interroger la Commission sur la légalité d'une éventuelle interception administrative. Il convient de préciser que nombre de requérants se sont adressés à la CNCIS téléphoniquement avant toute démarche écrite. Ce contact préalable a le plus souvent permis de prévenir des courriers ultérieurs inappropriés lorsqu'il s'agit d'appels malveillants, de problèmes relevant de la saisine de l'autorité judiciaire (soupçons d'écoutes illégales à caractère privé) ou enfin de dysfonctionnements techniques classiques ; il a également permis de réorienter les demandeurs vers les services ou autorités compétents.

Il convient de rappeler que le pouvoir d'investigation exercé sur le fondement de l'article 15 a été précisé par le Conseil d'État dans un arrêt du 28 juillet 1999 (CNCIS, 9<sup>e</sup> rapport, p. 34). Aux termes de cet arrêt, ce pouvoir ne saurait être étendu à l'origine des informations ayant déclenché une action des services de police.

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

La CNCIS n'a pas eu à user des dispositions du 2<sup>e</sup> 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.

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

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

## Le contrôle du matériel

À l'occasion de son dixième anniversaire, la Commission a rappelé le processus qui avait conduit à la mise en place puis à la modification des textes réglementaires régissant les matériels d'écoute (CNCIS, 10<sup>e</sup> rapport 2001, p. 25). On peut s'y reporter utilement. Rappelons simplement ici le cadre juridique. Il se résume à quatre séries de textes : tout d'abord, l'article 226-3 du Code pénal qui dispose que « est punie des mêmes peines (un an d'emprisonnement et de 45 000 euros d'amende ; *cf.* art 226-1 du Code pénal) la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente, en l'absence d'autorisation ministérielle dont les conditions d'octroi sont fixées par décret en Conseil d'État, d'appareils conçus pour réaliser les opérations pouvant constituer l'infraction prévue par le deuxième alinéa de l'article 226-15 ou qui, conçus pour la détection à distance des conversations, permettent de réaliser l'infraction prévue par l'article 226-1 et figurant sur une liste dressée dans des conditions fixées par ce même décret [...] » ; ensuite, les articles R. 226-1 à -12 du même Code, qui organisent les conditions et modalités de délivrance des autorisations ; puis l'arrêté du 9 mai 1994 fixant la liste des appareils prévue à l'article 226-3, repris ci-dessus ; et enfin l'arrêté du 15 janvier 1998 relatif au registre visé par l'article R. 226-10.

En 2003, la commission consultative compétente pour donner les avis sur les demandes d'acquisition/détention ou commercialisation des matériels visés par cette réglementation s'est réunie sept fois. Sa composition est la suivante :

- le secrétaire général de la défense nationale ou son représentant, président ;
- un représentant du ministre de la Justice ;
- un représentant du ministre de l'Intérieur ;
- un représentant du ministre de la Défense ;
- un représentant du ministre chargé des Douanes ;

- un représentant du ministre chargé de l'Industrie ;
- un représentant du ministre chargé des Télécommunications ;
- un représentant de la Commission nationale de contrôle des interceptions de sécurité ;
- un représentant du directeur général de l'Agence nationale des fréquences ;
- deux personnalités désignées en raison de leurs compétences, par le Premier ministre.

735 dossiers ont été présentés en 2003, 375 pour les demandes initiales et 360 pour les renouvellements. Concernant chacun un ou plusieurs matériels, ils ont donné lieu à la délivrance de 1264 autorisations et à deux refus relatifs à des demandes d'acquisition/détention.

On assiste ici à travers une augmentation du nombre total d'autorisations délivrées à un double phénomène : d'une part, le tassement continu des demandes nouvelles attestant que la période de régularisation depuis l'entrée en vigueur des textes réglementaires est échue et que la Commission ne traite plus que le flux ; d'autre part, la montée en puissance des demandes de renouvellement d'autorisations à échéance (360 contre 84 en 2002), qui explique à elle seule l'augmentation du nombre total d'autorisations mettant fin au tassement progressif de ce dernier observé depuis deux ans.

En dehors de sa participation à la commission consultative, la préoccupation de la CNCIS au sujet des matériels se concrétise également par des visites directes chez les fabricants ou les revendeurs ou à l'occasion de salons spécialisés comme le salon « Milipol ».

Ces déplacements comportent une part de veille technologique mais ils sont aussi pour la CNCIS un moyen de connaître l'état du marché. En effet, au-delà du suivi exhaustif des demandes d'interceptions présentées par les services, la Commission estime devoir contribuer à la protection de la vie privée en participant à la lutte contre les tentatives de contournements de la loi constituées notamment par les écoutes dites « sauvages ».

Dans cet esprit, certains services de l'État, titulaires d'autorisations de « plein droit » conformément au régime mis en place en 2001, sont invités à produire leurs registres et à décrire leurs règles internes de gestion des matériels sensibles. Ces rencontres permettent aux représentants de la CNCIS de s'assurer du respect des règles adoptées et de l'adéquation des matériels achetés avec les missions des services.

En fait, et cette affirmation n'est pas nouvelle, la vraie menace d'atteinte à la vie privée vient d'individus ou officines peu scrupuleux. Il peut être en effet facile, étant animé de mauvaises intentions, de se procurer des appareils tournant la réglementation française, notamment grâce à l'internet ou en jouant sur les différences de régime juridique au sein de l'Union européenne et sur la liberté de circulation des personnes et des biens. Précisément la réglementation européenne va conduire à des révisions internes. Le système français a, dans sa rigueur même que la CNCIS approuve,

contrevenu pour partie à la réglementation européenne. Dans le cadre de la phase précontentieuse opposant la France à la Commission européenne sur la question des « scanners », une modification de l'arrêté de 1994, convenue d'un commun accord avec l'ensemble des membres de la Commission dite R226, et fondée sur le principe de la proportionnalité (simple déclaration sur les matériels de faible dangerosité, régime d'autorisation maintenu pour les matériels réellement sensibles) est en gestation.

## Actualités de l'année 2003

Dans son précédent rapport d'activité (11<sup>e</sup> rapport 2002, p. 97*et sq.*) la CNCIS a évoqué le souci des autorités belges d'adopter une législation en vue d'autoriser les interceptions de sécurité. Des contacts avaient été noués fin 2002 entre le « Comité R », institution belge dont la mission principale consiste en un contrôle des services de renseignements et la CNCIS. Dans l'optique de l'adoption d'une telle législation, le « Comité R » se verrait vraisemblablement confier la mission de contrôle des interceptions dévolue en France à la CNCIS. Une délégation belge composée de M. Jean-Claude Delepierre, président du Comité R, MM. Gérard Van de Walle et Walter De Smedt, conseillers, et de M. Wouter De Ridder, greffier, a été reçue par la CNCIS le 4 avril 2003 pour une présentation de l'expérience française.

Le 6 mai 2003 une présentation des interceptions de sécurité et de la CNCIS a été faite à une délégation composée de responsables du ministère de la Justice italienne, ce pays ne connaissant que les interceptions judiciaires.

Enfin, le 20 juin 2003 la CNCIS a présenté le modèle français à une délégation japonaise conduite par M. le professeur Masao Horibe, président du groupe d'études sur le secret des correspondances émises par la voie de télécommunications.

Deuxième partie

# ÉTUDES ET DOCUMENTS

# Présentation ordonnée des textes relatifs aux interceptions

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

Les interceptions de correspondances émises par la voie des télécommunications sont de deux types, judiciaires et de sécurité. S'agissant des interceptions judiciaires, le pluriel est employé à dessein depuis l'intervention de la loi n° 2002-1138 du 9 septembre 2002.

En effet, aux interceptions en matière criminelle et correctionnelle prévues par les art. 100 et 100-7 du Code de procédure pénale, s'ajoutent désormais celles prévues par l'art. 80-4 du même code dans le cadre de l'information ouverte pour recherche des causes de la mort ou d'une disparition de mineur, de majeur protégé ou présentant un caractère inquiétant. Avant d'exposer les dispositions spécifiques ou communes aux différents types d'interception, il convient de rappeler le principe du secret des correspondances émises par la voie des télécommunications posé par l'article 1<sup>er</sup> de la loi n° 91-646 du 10 juillet 1991 : « Le secret des correspondances émises par la voie des télécommunications est garanti par la loi. Il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci. »

## Les interceptions ordonnées par l'autorité judiciaire

### Les interceptions ordonnées en matière criminelle et correctionnelle

Code de procédure pénale : livre premier. De l'exercice de l'action publique et de l'instruction

Titre III. Des juridictions d'instruction

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

Sous-section 2. Des interceptions de correspondances émises par la voie des télécommunications (loi n° 91-646 du 10 juillet 1991 – Titre 1<sup>er</sup>)

#### **Art. 100.**

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

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

#### **Art. 100-1.**

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

#### **Art. 100-2.**

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

#### **Art. 100-3.**

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

#### **Art. 100-4.**

« Le juge d'instruction ou l'officier de police judiciaire commis par lui dresse procès-verbal de chacune des opérations d'interception et

d'enregistrement. Ce procès-verbal mentionne la date et l'heure auxquelles l'opération a commencé et celles auxquelles elle s'est terminée.

Les enregistrements sont placés sous scellés fermés. «

**Art. 100-5.**

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

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

**Art 100-6.**

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

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

**Art. 100-7. (loi n° 95-125 du 8 février 1995)**

« Aucune interception ne peut avoir lieu sur la ligne d'un député ou d'un sénateur sans que le président de l'assemblée à laquelle il appartient en soit informé par le juge d'instruction.

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

(Loi n° 93-1013 du 24 août 1993) « Les formalités prévues par le présent article sont prescrites à peine de nullité. »

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

**Art. 80-4** du Code de procédure pénale (loi n° 2002 -1138 du 9 sept. 2002, art. 66).

« Pendant le déroulement de l'information pour recherche des causes de la mort ou des causes d'une disparition mentionnée aux articles 74 et 74-1, le juge d'instruction procède conformément aux dispositions du chapitre 1<sup>er</sup> du titre III du livre 1<sup>er</sup>. Les interceptions de correspondances émises par la voie des télécommunications sont effectuées sous son autorité et son contrôle dans les conditions prévues au deuxième alinéa de l'article 100 et aux articles 100-1 à 100-7. Les interceptions ne peuvent excéder une durée de deux mois renouvelable.

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

### **Les interceptions de sécurité (loi n° 91-646 du 10 juillet 1991 – Titre II)**

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

**Art. 4.** – L'autorisation est accordée par décision écrite et motivée du Premier ministre ou de l'une des deux personnes spécialement déléguées par lui. Elle est donnée sur proposition écrite et motivée du ministre de la Défense, du ministre de l'Intérieur ou du ministre chargé des Douanes, ou de la personne que chacun d'eux aura spécialement déléguée.

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

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

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

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

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

Cette transcription est effectuée par les personnels habilités.

**Art. 8.** – Il est établi, sous l'autorité du Premier ministre, un relevé de chacune des opérations d'interception et d'enregistrement. Ce relevé

mentionne la date et l'heure auxquelles elle a commencé et celles auxquelles elle s'est terminée.

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

Il est dressé procès-verbal de cette opération.

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

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

**Art. 11-1.** – *(introduit par l'article 31 de la loi 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne)*

Les personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité sont tenues de remettre aux agents autorisés dans les conditions prévues à l'article 4, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies. Les agents autorisés peuvent demander aux fournisseurs de prestations susmentionnés de mettre eux-mêmes en œuvre ces conventions, sauf si ceux-ci démontrent qu'ils ne sont pas en mesure de satisfaire à ces réquisitions.

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

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

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

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

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

**Art. 13.** – Il est institué une Commission nationale de contrôle des interceptions de sécurité. Cette Commission est une autorité administrative indépendante. Elle est chargée de veiller au respect des dispositions du présent titre. Elle est présidée par une personnalité désignée, pour une durée de six ans, par le président de la République, sur une liste de quatre noms établie conjointement par le vice-président du Conseil d'État et le premier président de la Cour de cassation.

Elle comprend, en outre :

- un député désigné pour la durée de la législature par le président de l'Assemblée nationale ;
- un sénateur désigné après chaque renouvellement partiel du Sénat par le président du Sénat.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Art. 19.** – La Commission remet chaque année au Premier ministre un rapport sur les conditions d'exercice et les résultats de son activité, qui précise notamment le nombre de recommandations qu'elle a adressées au Premier ministre en application de l'article 14 et les suites qui leur ont été données. Ce rapport est rendu public.

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

### **Dispositions communes aux interceptions judiciaires et de sécurité (loi n° 91-646 du 10 juillet 1991 – Titre III)**

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

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

**Art. 22.** – *(modifié par l'article 18 de la loi n° 96-659 du 26 juillet 1996 sur la réglementation des télécommunications)*

Les juridictions compétentes pour ordonner des interceptions en application du Code de procédure pénale ainsi que le Premier ministre ou, en ce qui concerne l'exécution des mesures prévues à l'article 20, le ministre de la Défense ou le ministre de l'Intérieur, peuvent recueillir, auprès des personnes physiques ou morales exploitant des réseaux de télécommunications ou fournisseurs de services de télécommunications ou l'organisme visé à l'article L. 35-4 du Code des postes et télécommunications, les informations ou documents qui leur sont nécessaires, chacun en ce qui le concerne, pour la réalisation et l'exploitation des interceptions autorisées par la loi.

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

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

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

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

**Article 226-3.** – Est puni des mêmes peines [un an d'emprisonnement et 45 000 euros d'amende] la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente, en l'absence d'autorisation ministérielle dont les conditions d'octroi sont fixées par décret en Conseil d'État,

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

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

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

Est puni des mêmes peines le fait, par une personne visée à l'alinéa précédent ou un agent d'un exploitant de réseau de télécommunications autorisé en vertu de l'article L. 33-1 du Code des postes et télécommunications ou d'un fournisseur de services de télécommunications, agissant dans l'exercice de ses fonctions, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu.

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

**Art. 26.** – Sera punie des peines mentionnées à l'article 226-13 <sup>1</sup> du Code pénal toute personne qui, concourant dans les cas prévus par la loi à l'exécution d'une décision d'interception de sécurité, révélera l'existence de l'interception.

**Art. 27.** – La présente loi entrera en vigueur le 1<sup>er</sup> octobre 1991.

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

## Textes réglementaires récents visant la loi du 10 juillet 1991

Deux décrets méritent d'être soulignés. Le premier en date du 12 avril 2002 a trait à l'érection en service du groupement interministériel de contrôle et consacre le principe de centralisation des interceptions fixé par l'article 4 de la loi du 10 juillet 1991. Le second en date du 16 juillet 2002 tend à mettre en œuvre les obligations pesant sur les fournisseurs de prestations de cryptologie introduites par l'article 11-1 de la loi du 10 juillet 1991.

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

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

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

**Art. 2.** – Le groupement interministériel de contrôle a pour mission :

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

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

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

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

**Art. 1<sup>er</sup>.** – L'obligation mise à la charge des fournisseurs de prestations de cryptologie par l'article 11-1 de la loi du 10 juillet 1991 susvisée

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

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

**Art. 2.** – Les décisions prises en application de l'article 1<sup>er</sup> sont notifiées au fournisseur de prestations de cryptologie et communiquées sans délai au président de la Commission nationale de contrôle des interceptions de sécurité.

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

**Art. 4.** – La décision mentionnée au premier alinéa de l'article 1<sup>er</sup> :

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

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

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

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

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

## Actualité législative

### Télécommunications

On relève ici seulement la loi n° 2003-1365 du 31 décembre 2003, relative aux obligations de service public des télécommunications et à France Télécom. Cette loi, transposant en droit interne des dispositions de la directive 2002/77/CE du 16 septembre 2002 de la Commission relative à la concurrence dans les marchés de réseaux et des services de communications électroniques et de la directive 2002/22/CE du 7 mars 2002 du Parlement européen et du Conseil concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications. Il s'agit pour 2003 de la seule transposition en droit interne de l'ensemble des directives européennes constituant ce qu'il est convenu d'appeler le « Paquet Télécom ».

### Procédure pénale

La loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la grande criminalité comporte plusieurs dispositions relatives aux interceptions de correspondances émises par la voie des télécommunications. Publiée au premier trimestre 2004, le processus législatif a intéressé toute l'année 2003, ce qui justifie sa place dans le présent rapport. Il est utile de rappeler les dispositions préexistantes et d'évoquer celles qui viennent d'être adoptées.

### Les dispositions préexistantes

Aux termes des articles 100 à 100-7 du Code de procédure pénale constituant le titre 1<sup>er</sup> de la loi du 10 juillet 1991 « en matière criminelle et en

matière correctionnelle, si la peine encourue est égale ou supérieure à deux ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, ordonner l'interception (...) de correspondances émises par la voie des télécommunications » (art. 100).

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

Aux termes de l'art. 66 du Code de procédure pénale tel qu'il résulte de l'art 80-4 de la loi n° 2002-1138 du 9 septembre 2002, « pendant le déroulement de l'information pour recherche des causes de la mort ou des causes d'une disparition mentionnée aux articles 74 et 74-1, le juge d'instruction procède conformément aux dispositions du chapitre 1<sup>er</sup> du titre III du livre 1<sup>er</sup>. Les interceptions de correspondances émises par la voie des télécommunications sont effectuées sous son autorité et son contrôle dans les conditions prévues au deuxième alinéa de l'art 100 et aux articles 100-1 à 100-7. Les interceptions ne peuvent excéder une durée de **deux mois renouvelable** ».

### Les nouvelles dispositions

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

« 1° personne faisant l'objet d'un mandat d'arrêt délivré par le juge d'instruction, le juge des libertés et de la détention, la chambre de l'instruction ou son président ou le président de la cour d'assises, alors qu'elle est renvoyée devant une juridiction de jugement ;

« 2° personne faisant l'objet d'un mandat d'arrêt délivré par une juridiction de jugement ou par le juge de l'application des peines ;

« 3° personne condamnée à une peine privative de liberté sans sursis supérieure ou égale à un an, lorsque cette condamnation est exécutoire ou passée en force de chose jugée.

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

« **Art. 706-95.** du Code de procédure pénale – Si les nécessités de l'enquête de flagrance ou de l'enquête préliminaire relative à l'une des

infractions entrant dans le champ d'application de l'article 706-73 l'exigent, le juge des libertés et de la détention du tribunal de grande instance peut, à la requête du procureur de la République, autoriser l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications selon les modalités prévues par les articles 100 deuxième alinéa, 100-1 et 100-3 à 100-7, pour une durée maximum de **quinze jours, renouvelable une fois** dans les mêmes conditions de forme et de durée. Ces opérations sont faites sous le contrôle du juge des libertés et de la détention (...).

Ces dispositions complétées de celles relatives aux interceptions de sécurité et des évolutions successives au cours de la procédure parlementaire peuvent être synthétisées sous la forme du tableau suivant. «

### Interceptions judiciaires et de sécurité

Tableau récapitulatif des durées d'interceptions et conditions de renouvellement

|                           | Autorité                                                        | Motif                                                                                                                          | Durée    | Renouvellement                                                                             |
|---------------------------|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|----------|--------------------------------------------------------------------------------------------|
| Interceptions de sécurité | Premier ministre                                                | Prévention<br>– terrorisme<br>– criminalité organisée<br>– sécurité nationale<br>– protection économique<br>– ligues dissoutes | 4 mois   | Sans limitation                                                                            |
| Interceptions judiciaires | Juge d'instruction                                              | Matière criminelle et correctionnelle (peine encourue supérieure à deux ans)                                                   | 4 mois   | Sans limitation                                                                            |
|                           | Juge d'instruction                                              | Recherche des causes de la mort ou de disparitions inquiétantes                                                                | 2 mois   | Sans limitation                                                                            |
|                           | Parquet sous l'autorité du juge des libertés et de la détention | Recherche de personnes en fuite                                                                                                | 2 mois   | Renouvelable trois fois en matière correctionnelle ; sans limitation en matière criminelle |
|                           | Parquet (sous l'autorité du JLD)                                | Criminalité organisée                                                                                                          | 15 jours | Renouvelable une fois                                                                      |

### Observations

La lecture de ce tableau récapitulatif fait apparaître une diversification accrue des délais et des modes de renouvellement des interceptions, justifiée, pour le législateur, par la différence de motifs et d'autorités responsables de la décision. Ces différents délais et procédures devront être gérés sans erreur par la chaîne des décideurs et par les opérateurs de télécommunications.

## Réflexions sur le motif d'interception « sécurité nationale »

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

À la lumière des interceptions de nature diverse sollicitées sous ce motif, il paraît intéressant de réfléchir sur le contenu du concept de sécurité nationale, son évolution et ses limites.

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

Dans un premier temps, on s'attachera à rechercher dans l'élaboration de la loi toute précision sur l'origine du concept.

### L'origine du concept

#### **Exposé des motifs du projet de loi**

Il y est dit que la notion de sécurité nationale « recouvre, pour le Gouvernement, l'ensemble des informations qu'il juge nécessaire de détenir : 1) pour assurer la sauvegarde de la sécurité intérieure et extérieure du pays ; l'intégrité du territoire ; la vie de la population ;

2) pour prévenir les atteintes à la sûreté de l'État au sens du Code pénal dans sa rédaction actuelle (articles 70 à 103) « .

L'examen de la procédure parlementaire livre une précision importante sur l'origine du concept mais n'apporte que peu d'éclairage sur son contenu.

### Rapport de la commission des lois du Sénat

« La notion de sécurité nationale est préférée à celle d'atteinte à la sûreté intérieure et extérieure de l'État (...). La sécurité nationale, notion qui n'existe pas en tant que telle dans le droit français, est directement empruntée à l'article 8 de la Convention européenne<sup>1</sup>. Elle recouvre la Défense nationale ainsi que les autres atteintes à la sûreté et à l'autorité de l'État qui figurent au début du titre premier du livre troisième du Code pénal. »

### Débats à l'Assemblée nationale

M. Jacques Toubon qui avait déjà déposé une proposition de loi parallèle présenta un amendement ainsi libellé : « Les interceptions de sécurité publique ne sont autorisées que dans les cas suivants :

- recherche de renseignements intéressant la sécurité extérieure et intérieure de la France ;
- prévenir des atteintes à la sécurité publique extérieure et intérieure de l'État. »

L'amendement fut repoussé (*JOAN*, 2<sup>e</sup> séance du 13 juin 1991, p. 3152 et 3153).

### Débats au Sénat

M. Jacques Thyraud intervint dans les termes suivants : « Le texte du projet de loi emploie les termes inhabituels de *sécurité nationale*. Certes, cette terminologie est utilisée dans la Convention européenne des droits de l'homme. Cependant, alors qu'il est déjà difficile de définir les notions de sûreté de l'État ou de sécurité publique, il ne me paraît pas judicieux de faire figurer dans notre législation le nouveau concept de sécurité nationale pour lequel se posera encore un problème de définition. C'est pourquoi je propose de recourir à l'expression de *sûreté de l'État* qui figure habituellement dans nos textes. »

1) Article 8 : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui dans une société démocratique est nécessaire à la sécurité nationale, à la sûreté publique (...). »

M. Marcel Rudloff, rapporteur, apaisa M. Thyraud qui retira son amendement après les explications suivantes : « Si la Commission pense que M. Thyraud a raison de s'inquiéter, elle considère toutefois que, s'agissant d'un concept nouveau qui sera mis en vigueur par une commission non judiciaire, il n'est pas mauvais d'employer une autre expression que pour les poursuites pénales. C'est la raison pour laquelle la Commission estime qu'il faut maintenir les termes de *sécurité nationale* qui sont, comme on l'a rappelé, conformes à la Convention européenne des droits de l'homme, et qu'il ne convient donc pas de les remplacer par les mots *sûreté de l'État*, qui concernent, eux, le droit pénal. »

On le voit, c'est délibérément qu'a été choisi le concept de sécurité nationale pour définir un des motifs légaux d'interceptions. Ce choix s'explique par l'article 8 de la Convention européenne qui fonde le droit à une vie privée et les atteintes exceptionnelles qui peuvent y être portées. En ce sens l'article 8 de la Convention européenne a trouvé si l'on peut dire sa transposition en droit interne sous la forme des articles 1<sup>er</sup> et 3<sup>e</sup> de la loi du 10 juillet 1991.

## Le contenu du concept

Voilà pour l'origine du concept. Il convient maintenant de tenter d'en préciser le contenu. Même si M. Rudloff a expliqué que le concept ne devait rien au droit pénal dont il convenait de s'écarter, on notera que, dans l'exposé des motifs, référence au Code pénal continuait d'être faite à propos des informations que « le gouvernement juge nécessaire de détenir pour prévenir les atteintes à la sûreté de l'État au sens du Code pénal dans sa rédaction actuelle (articles 70 à 103) ».

On s'attachera donc à établir la liste des atteintes incriminées dans ces articles de l'ancien Code pénal qui définissent, « en creux », la sûreté de l'État.

Les articles 70 à 85 visent la trahison et l'espionnage ; les articles 86 à 92 les attentats, complots et autres infractions contre l'autorité de l'État et l'intégrité du territoire national ; les articles 93 à 96, les crimes tendant à troubler l'État par le massacre et la dévastation ; les articles 97 à 99, les crimes commis par la participation à un mouvement insurrectionnel ; les articles 100 à 103 regroupent des notions diverses (exemption de peine, non-dénonciation de crime).

Ces articles sont aujourd'hui abrogés mais les incriminations se retrouvent globalement dans l'actuel livre IV du Code pénal constituant désormais les « atteintes aux intérêts fondamentaux de la nation ».

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

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

S'agissant de la sauvegarde des éléments essentiels du potentiel scientifique et économique, celle-ci est assurée dans la loi de 1991 par un motif autonome, distinct de celui de la sécurité nationale. Pour ce qui concerne la sauvegarde du milieu naturel et du patrimoine culturel, on notera qu'aucun des articles suivants et sensés réprimer les atteintes aux intérêts fondamentaux listés à l'art. 410-1 du Code pénal ne s'y réfère.

Les intérêts fondamentaux susceptibles de recouvrir le concept de sécurité nationale, seraient donc constitués par l'énumération de l'art. 410-1 allant de l'indépendance de la nation à la sauvegarde de la population en France et à l'étranger (à cet égard, la sauvegarde d'un seul de nos ressortissants à l'étranger fait bien partie des intérêts fondamentaux de la nation).

Ces intérêts fondamentaux font l'objet d'atteintes incriminées aux art. 411-1 à 414-9 du Code pénal qui, globalement comme on l'a dit, sont une reprise des crimes contre la sûreté de l'État du premier chapitre du livre 3<sup>e</sup> de l'ancien Code pénal (art. 70 à 103).

On y retrouve notamment :

- la trahison et l'espionnage (art. 411-1 à 411-11) ;
- les autres atteintes aux institutions de la République ou à l'intégrité du territoire national : l'attentat et le complot (art. 412-1 et 412-2) ; le mouvement insurrectionnel (art. 412-3 à 412-6) ; l'usurpation de commandement, la levée de forces armées et la provocation à s'armer illégalement (art. 412-7 et 412-8).
- les autres atteintes à la Défense nationale comprenant : les atteintes à la sécurité des forces armées et aux zones protégées intéressant la Défense nationale (art. 413-1 à 413-8) ; les atteintes au secret de la Défense nationale (art. 413-9 à 413-12) ;
- des dispositions particulières sur les peines, leur exemption ou leur réduction (art. 414-1 à 414-9).

La différence notable avec l'ancien Code pénal tient à la distinction désormais opérée entre les atteintes aux intérêts fondamentaux perpétrées contre la nation en temps de paix incriminées dans le Code pénal et celles perpétrées en temps de guerre qui sont désormais insérées dans le Code de justice militaire, livre troisième, titre III, « Des atteintes aux intérêts fondamentaux de la nation en temps de guerre (art. 476-1 à 476-16).

Malgré la nouveauté du concept d'intérêts fondamentaux de la nation, la doctrine considère qu'il y a bien « maintien de la fusion de la sûreté extérieure et de la sûreté intérieure en une notion unique, la sûreté de l'État,

effectuée par l'ordonnance du 4 juin 1960, mais camouflée dans le nouveau code sous le couvert de la notion polymorphe des intérêts fondamentaux de la nation » (André Vitu, *Jurisclasseur pénal*, rubrique art. 410-1, « atteintes aux intérêts fondamentaux de la nation », paragraphe 57).

## Les observations de la Commission sur le motif d'interception « sécurité nationale »

Assez rapidement (rapport d'activité 1994, p. 17 *et sq.*), la CNCIS a estimé que « la notion de sécurité nationale devait être comprise au vu des nouvelles dispositions du Code pénal qui fait figurer la sécurité parmi les intérêts fondamentaux de la nation (art. 410-1 du Code pénal) au même titre que l'intégrité du territoire, la forme républicaine des institutions ou les moyens de la défense.

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

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

Ces observations ont été réitérées et complétées comme suit dans le même rapport (p. 36) :

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

La Commission est restée fidèle à cette doctrine.

S'agissant des troubles à l'ordre public, de temps à autre, peuvent être présentées des demandes motivées par cette crainte, sans que soit cependant allégué le risque d'attenter à la forme républicaine des institutions ou de déboucher sur un mouvement insurrectionnel. Si des manifestations sont susceptibles de dégénérer, le droit de manifester étant constitutionnellement reconnu, il s'agit là, en principe, d'un problème d'ordre public et non d'atteinte à la sécurité nationale. Il est toutefois possible que, par la charge symbolique, voulue le plus souvent par ses auteurs, affectant le *lieu* et le *temps* de la manifestation et la qualité des autorités

visées, le risque d'atteinte aux institutions <sup>1</sup> et, en tout cas, de menace de la sécurité intérieure soit avéré.

S'agissant de la recherche de renseignements sur la situation politique prévalant dans un pays tiers, la personne dont on se propose d'intercepter les correspondances doit être suspectée d'attenter par ses agissements aux intérêts fondamentaux de la nation. Si les services de renseignements ont, par nature, une mission de collecte de renseignements par utilisation de la palette des sources disponibles, les interceptions de sécurité doivent toutefois faire exception. En effet, l'atteinte exceptionnelle à la vie privée qu'autorise la loi ne peut être justifiée que par la menace que la personne écoutée représente pour la sécurité nationale. En l'absence de menace, et quel que soit l'intérêt que représente la cible comme source de renseignement pour le domaine considéré, l'atteinte à la vie privée serait contraire au principe de proportionnalité et l'avis de la Commission ne pourrait être que défavorable. Cette observation vaut naturellement pour les autres motifs légaux d'interception comme la prévention du terrorisme et la lutte contre la criminalité organisée même si, pour ces derniers, l'implication de la cible dans le processus conspiratif ou criminel a toujours été avérée.

---

1) Cf. l'exemple historique des affrontements du 6 février 1934, pont de la Concorde, face à l'Assemblée nationale.

## Réflexions sur le motif d'interception « protection économique »

La sauvegarde des éléments essentiels du potentiel scientifique et économique de la France plus communément et rapidement nommée « protection économique » est le motif d'interception le plus faible en volume, à l'exception de la reconstitution de ligues dissoutes pour lequel le chiffre est nul depuis de nombreuses années.

Cependant c'est le motif qui lors de la discussion parlementaire de la loi du 10 juillet 1991 a suscité le plus de réserves.

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

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

Les débats parlementaires livrent encore les précisions suivantes : « La possibilité d'interceptions de sécurité pour la protection des intérêts économiques et scientifiques fondamentaux d'un État est reconnue par la Convention européenne des droits de l'homme, dont le texte est d'ailleurs moins restrictif que le projet de loi, puisqu'il se réfère à la notion de

« bien-être économique. » <sup>1</sup> Les interceptions autorisées à ce titre viseront, par exemple, à prévenir les risques liés à la prolifération de technologies sensibles et il est nécessaire que l'État dispose de moyens d'information et d'action adaptés aux **menaces** résultant de l'internationalisation des activités économiques » (François Massot, rapport de la commission des lois de l'Assemblée nationale, 6 juin 1991, Document n° 2088, p. 29).

Qu'entend-on par « sauvegarde des éléments essentiels du potentiel scientifique et économique de la nation » au sens du Code pénal ? Celle-ci fait partie des intérêts fondamentaux de la nation tels que définis par l'article 410-1 du Code pénal.

## Les intérêts fondamentaux de la nation

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

Comme il a été dit plus haut, cet article inaugure le titre premier du livre IV « Des crimes et délits contre la nation, l'État, et la paix publique ». L'art. 410-1 ne définit d'ailleurs pas à proprement parler la notion d'intérêts fondamentaux de la nation, se bornant à en donner une énumération qui a d'ailleurs été inutilement allongée au fil de la procédure parlementaire, comme l'indique André Vitu dans le commentaire qu'il donne de cet article au sein de la rubrique *ad hoc* du *Jurisclasseur pénal*. En effet, cette énumération donne la liste des intérêts fondamentaux qui font l'objet de protections spécifiques et donc d'incriminations dans les articles suivants : 411-1 à 411-11. Or, par exemple, aucune incrimination, du moins dans le livre IV du Code pénal, n'assure aux art. 411-1 à 411-11 la protection du milieu naturel et de l'environnement.

---

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

## La sauvegarde des éléments essentiels du potentiel scientifique et économique de la nation

Au titre des intérêts fondamentaux de la nation est donc retenue la sauvegarde des éléments essentiels de son potentiel scientifique et économique « et de son patrimoine culturel », ce dernier ajout ayant été fait par le Parlement contre l'avis du Gouvernement. Cette formulation « permet d'étendre **la protection du Code pénal** non seulement aux différents secteurs de l'économie au sens étroit du terme mais également à la recherche scientifique et aux innovations techniques ou technologiques sur lesquelles reposent précisément la force ou la compétitivité du pays » (A. Vitu, *op. cité*).

## Les atteintes aux éléments essentiels du potentiel scientifique et économique de la nation

Après la définition des intérêts fondamentaux de la nation, à l'art. 410-1 du Code pénal, suivent les articles 411-1 à 411-11 qui incriminent les différentes atteintes à ces intérêts. Parmi celles-ci sont plus spécialement intéressantes les infractions des articles 411-5 à 411-8 relatives aux intelligences avec une puissance étrangère (art. 411-5) et à la livraison d'informations à celle-ci (art. 411-6 à 411-8).

« **Art. 411-5** – Le fait d'entretenir des intelligences avec une puissance étrangère, avec une entreprise ou organisation étrangère ou sous contrôle étranger ou avec leurs agents, lorsqu'il est de nature à porter atteinte aux intérêts fondamentaux de la nation, est puni de dix ans d'emprisonnement et de 150 000 euros d'amende.

**Art. 411-6** – Le fait de livrer ou de rendre accessibles à une puissance étrangère, à une entreprise ou organisation étrangère ou sous contrôle étranger à leurs agents des renseignements, procédés, objets, documents, données informatisées ou fichiers dont l'exploitation, la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la nation est puni de quinze ans de détention criminelle et de 225 000 euros d'amende.

**Art. 411-7** – Le fait de recueillir ou de rassembler, en vue de les livrer à une puissance étrangère, à une entreprise ou organisation étrangère ou sous contrôle étranger ou à leurs agents, des renseignements, procédés, objets, documents, données informatisées ou fichiers dont l'exploitation, la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la nation est puni de dix ans d'emprisonnement et de 150 000 euros d'amende.

**Art. 411-8** – Le fait d'exercer, pour le compte d'une puissance étrangère, d'une entreprise ou organisation étrangère ou sous contrôle étranger ou de leurs agents, une activité ayant pour but l'obtention ou la livraison de dispositifs, renseignements, procédés, objets, documents, données informatisées ou fichiers dont l'exploitation, la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la nation est puni de dix ans d'emprisonnement et de 150 000 euros d'amende. »

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

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

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

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

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

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

Il résulte de ce qui précède que la sauvegarde des éléments essentiels du potentiel scientifique et économique de la nation suppose une suspicion d'atteinte à ce potentiel, une menace, et que la cible dont on se propose d'écouter les communications soit impliquée dans cette menace.

---

1) Le terme entreprise étant ici entendu non au sens « d'entreprise terroriste » comme dans l'art. 421-1 du Code pénal, mais bien au sens du droit commercial du droit du travail et de l'économie politique à savoir la réunion des facteurs de production du capital et du travail nécessaires à la mise en œuvre d'une activité professionnelle déterminée.

## Interceptions de sécurité et secret défense

La publication de l'arrêté du 25 août 2003 relatif à la protection du secret de la défense nationale et portant instruction générale interministérielle sur la protection du secret de la défense nationale, est l'occasion de réaffirmer les fondements de la protection attachée aux interceptions de sécurité. Aux termes de l'article 2 de l'arrêté susvisé, « présentent un caractère de secret de la défense nationale au sens des articles 413-9 et suivants du Code pénal les renseignements, procédés, objets, documents, données informatisées ou fichiers :

- intéressant la défense nationale qui ont fait l'objet de mesures de protection destinées à restreindre leur diffusion ;
- dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale.

Pris en application des dispositions du dernier alinéa de l'art. 413-9 du Code pénal, le décret n° 98-608 du 17 juillet 1998 :

- définit trois niveaux de classification : Très Secret-Défense, Secret-Défense, Confidentiel-Défense ;
- prévoit que les informations ou supports protégés portent la mention de leur niveau de classification (...) « .

Les interceptions de sécurité relèvent des informations classifiées Secret-Défense : elles intéressent la **défense nationale** et sont revêtues de mention Secret-Défense.

La notion de secret de la défense nationale est définie par l'article 2 de l'arrêté du 25 août 2003. La classification « secret-défense » d'un document ou d'une information répond à deux exigences cumulatives :

- une exigence de fond : l'information ou le document doit intéresser la défense nationale ;
- une exigence de forme : l'apposition de la mention « secret-défense ».

La notion de défense nationale doit être entendue largement. Elle trouve sa définition dans l'article 1 de l'ordonnance 59-147 du 07 janvier 1959 portant organisation générale de la défense (ordonnance-cadre) : « La défense a pour objet d'assurer en tout temps, en toutes circonstances et contre toutes les formes d'agression, la sécurité et l'intégrité du territoire, ainsi que la vie de la population. »

Le rapport d'activité 2001-2003 de la Commission nationale consultative du secret de la défense nationale éclaire cette définition en ces termes : « La défense s'exerce, comme le stipule l'ordonnance de 1959 en tous temps et en tous lieux, et concerne tous les secteurs d'activité ; défense militaire du pays, mais aussi défense civile, sécurité intérieure, protection des activités financières, économiques ou industrielles, protection du patrimoine scientifique et culturel de la France ».

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

La classification « Secret-Défense » de tous les éléments relatifs à une interception de sécurité (et quel qu'en soit le motif au regard de l'ordonnance de 1959 qui préfigure la notion « d'intérêts fondamentaux de la nation de l'article 410-1 du Code pénal qui recouvre elle même le domaine de l'article 3 de la loi du 10 juillet 1991) s'impose donc. Par conséquent, la position prise par la CNCIS depuis ses débuts, d'appliquer à la lettre <sup>1</sup> l'article 17 de la loi du 10 juillet 1991 (notamment la non-information des particuliers de l'existence ou la non-existence d'une interception de sécurité) est bien conforme à l'ensemble de l'architecture normative concernant le secret de la défense nationale qui doit être protégé en toutes circonstances tant qu'il n'est pas levé.

---

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

# Jurisprudence

## Jurisprudence européenne

### Procès équitable

Auto-incrimination – obtention d’une confession par un informateur de la police placé dans la cellule du suspect : violation.

***Arrêt ALLAN Royaume-Uni (n° 48539/99). Arrêt 5.11 2002 [Section IV] :***

En fait : pendant la détention provisoire du requérant, soupçonné de vol, avec un autre homme, G., leur cellule et le parloir qu’ils utilisaient furent placés sous surveillance audio et vidéo secrète par la police en liaison avec une enquête sur un meurtre. Des conversations entre les deux hommes et entre le requérant et sa visiteuse furent enregistrées. Par la suite, un informateur de la police, H., fut mis dans la cellule du requérant afin de lui soutirer des renseignements. H., qui avait été équipé d’un dispositif d’enregistrement, fit une déposition où il affirmait que le requérant avait avoué avoir été présent sur les lieux du crime. Cet aveu n’avait pas été enregistré et il n’existait aucune autre preuve établissant un lien entre le requérant et le meurtre. Au procès du requérant, son avocat contesta en vain la recevabilité des enregistrements secrets et du témoignage de H. Le requérant fut reconnu coupable et condamné à la réclusion criminelle à perpétuité. Il se vit refuser l’autorisation de faire appel.

En droit : article 8 – Il n’existait à l’époque des faits aucune disposition légale réglementant l’usage fait par la police de dispositifs d’enregistrement secrets ; l’ingérence n’était donc pas « prévue par la loi ».

Conclusion : violation (unanimité).

Article 6 (1) – Les enregistrements n'étaient pas illégaux au sens d'être contraires au droit pénal interne, et nul n'a laissé entendre que les aveux prononcés lors des conversations avec G. et la visiteuse aient été obtenus par la contrainte, ni qu'il y ait eu incitation policière ou financière. Il n'était pas facile d'apprécier la force ou la fiabilité des éléments de preuve en cause ; dans ces conditions, l'équité de la procédure revêtait une importance particulière. À cet égard, l'avocat du requérant a pu contester l'admissibilité des preuves, le juge du fond a rendu une décision soigneusement pesée et cette décision a été contrôlée en appel. La Cour n'est donc pas convaincue que l'utilisation au procès du requérant d'enregistrements de conversations qu'il avait eues avec G. et une visiteuse ait méconnu l'exigence d'équité énoncée à l'article 6. En revanche, la manière dont H. a été utilisé pour obtenir des preuves soulève des questions plus complexes. Le droit de garder le silence permet en principe à un suspect de choisir de s'exprimer ou de se taire lors d'un interrogatoire de police. Pareille liberté est effectivement mise à mal si les autorités recourent à des subterfuges pour soutirer des aveux ou autres déclarations à charge. En l'occurrence, les aveux qui auraient été faits à H. n'étaient pas spontanés mais avaient été provoqués par les questions continues de H. qui, à la demande de la police, avait orienté leurs conversations dans des conditions pouvant être considérées comme constituant l'équivalent d'un interrogatoire, mais sans les garanties qui accompagnent un véritable interrogatoire de police. Il n'existait aucune relation particulière entre le requérant et H. et il n'a pas été noté de contrainte directe, mais le requérant aura subi des pressions psychologiques portant atteinte au caractère volontaire de ses aveux. Dans ces conditions, les informations recueillies en recourant à H. de cette manière peuvent passer pour avoir été obtenues contre la volonté du requérant, et leur utilisation au procès pour avoir porté atteinte à son droit de garder le silence et de ne pas s'accuser lui-même.

Conclusion : violation (unanimité).

Article 13 – Le Gouvernement reconnaît que le requérant n'a pas disposé d'un recours effectif à l'époque des faits quant à ses griefs tirés de l'article 8.

Conclusion : violation (unanimité).

Article 41 – La Cour alloue au requérant 1642 euros pour dommage moral s'agissant des violations des articles 8 et 13 et juge que le constat de violation de l'article 6 (1) constitue une satisfaction équitable suffisante pour ce qui est du grief tiré de cet article. Elle octroie également une certaine somme pour frais et dépens.

## **Vie privée**

Lecture, lors de l'audience, de retranscriptions de conversations téléphoniques interceptées dans le contexte de poursuites pénales et ultérieurement diffusées dans la presse : violation.

**Arrêt CRAXI c. Italie (n° 25337/94). Arrêt 17.7 2003 [Section I] :**

En fait : le requérant, ancien président du Conseil italien, fut renvoyé en jugement en juin 1994 pour corruption. Il s'enfuit en Tunisie. En septembre 1995, le tribunal de Milan autorisa l'interception de ses appels téléphoniques entre la Tunisie et l'Italie. Le procureur remit les procès-verbaux des conversations interceptées au greffe du tribunal et demanda qu'ils soient admis comme preuves. Le même jour, il procéda à la lecture d'extraits de ces conversations lors d'une audience. Les procès-verbaux furent mis à la disposition des parties immédiatement après. Des extraits d'un certain nombre de conversations interceptées parurent ensuite dans la presse, bien que personne n'ait reconnu les avoir divulgués. Le tribunal accepta un certain nombre de procès-verbaux comme preuves. Le requérant fut condamné.

En droit : article 8 – La lecture en audience puis la divulgation dans la presse ont constitué des ingérences dans le droit du requérant au respect de la vie privée et de la correspondance.

a) Divulgation : il est parfaitement compatible avec l'exigence de publicité des débats énoncée à l'article 6 de rendre compte de procédures judiciaires. Les médias ont le devoir de communiquer des informations et idées et le public a le droit d'en recevoir, en particulier lorsqu'elles concernent une personnalité connue. Cependant, l'intérêt public qu'il y a à recevoir des informations ne concerne que les faits en rapport avec les accusations en matière pénale dirigées contre l'accusé. En l'espèce, certaines des conversations parues dans la presse revêtaient un caractère strictement privé et n'avaient qu'un rapport ténu, voire aucun rapport, avec les accusations pénales. Leur publication par la presse ne correspondait donc à aucun besoin social impérieux et l'ingérence n'était pas proportionnée. Toutefois, il se pose la question de savoir si la responsabilité de l'État se trouvait engagée, la publication ayant été le fait de journaux privés et nul n'ayant laissé entendre qu'ils aient pu en quoi que ce soit se trouver placés sous le contrôle des autorités publiques. La Cour juge établi que les informations provenaient des procès-verbaux déposés au greffe du tribunal. Le procureur n'avait pas décidé de les faire tomber dans le domaine public, car, en droit interne, le dépôt d'un document au greffe le rend accessible, non au public, mais seulement aux parties. Dans ces conditions, la divulgation des conversations n'était pas la conséquence directe d'un acte du procureur mais plutôt le résultat d'un dysfonctionnement du greffe du tribunal ou de l'obtention par la presse des informations auprès de l'une des parties au procès ou de leurs avocats. À cet égard, il y a lieu de déterminer si les autorités ont pris les mesures qui s'imposaient pour assurer la protection effective des droits du requérant en mettant en place les garanties appropriées et en menant une enquête effective. Or les autorités ont failli à ces obligations.

Conclusion : violation (6 voix contre 1)

b) Lecture en audience : les exigences procédurales instaurées par le Code de procédure pénale visaient à fournir aux parties et au juge l'occasion

de choisir les conversations interceptées dépourvues de pertinence et dont la divulgation aurait porté atteinte au droit de l'accusé au respect de la vie privée et de la correspondance. Elles constituaient donc une protection importante. Or rien dans l'ordonnance du tribunal n'explique pourquoi ces garanties n'ont pu être respectées. Dans ces conditions, l'ingérence n'était pas « prévue par la loi », car les autorités n'ont pas suivi les procédures légales avant d'autoriser la lecture des procès-verbaux.

Conclusion : violation (unanimité).

Article 41 – La Cour alloue aux héritiers du requérant une somme au titre du dommage moral.

### Correspondance

Enregistrement d'une conversation téléphonique par une partie avec l'assistance de la police : violation.

#### ***Arrêt M.M. c. Pays-Bas (n° 39339/98). Arrêt 8.4 2003 [Section II] :***

En fait : le requérant, un avocat, fut amené à rencontrer S., la femme d'un de ses clients qui se trouvait en détention provisoire. S. déclara à son mari que le requérant lui avait fait des avances. Le mari de S. en informa la police, qui le signala à son tour au procureur. On suggéra à S. de brancher un magnétophone sur son téléphone afin qu'elle puisse enregistrer les appels provenant du requérant. Des policiers se rendirent chez elle pour effectuer le branchement et lui montrer comment se servir du magnétophone. Ils lui suggérèrent d'orienter la conversation sur le sujet des avances. Par la suite, la police emporta les enregistrements de plusieurs conversations. Le requérant fut reconnu coupable d'attentat à la pudeur. La cour d'appel annula ce jugement mais reconnut, elle aussi, le requérant coupable d'attentat à la pudeur, sans se fonder sur les enregistrements.

En droit : article 8 – Nul ne conteste que c'est la police qui a suggéré à S. d'enregistrer ses conversations avec le requérant. Avec l'autorisation du procureur, la police a branché un magnétophone sur le téléphone de S., lui a montré comment l'utiliser, lui a suggéré d'orienter la conversation sur le sujet des avances et, enfin s'est rendue au domicile de S. pour y chercher les enregistrements. Outre qu'elle était responsable de la conception de ce plan, la police a ainsi joué un rôle crucial dans l'exécution de celui-ci. À cette occasion, elle a agi, tout comme le procureur, dans l'exercice de ses fonctions officielles. La responsabilité de l'État était donc engagée et il y a eu ingérence d'une « autorité publique » dans le droit du requérant au respect de sa correspondance. À l'époque des faits, les écoutes téléphoniques ou l'interception de télécommunications demandaient une enquête judiciaire préliminaire et une décision du juge d'instruction, conditions dont aucune n'a été respectée en l'espèce. L'ingérence n'était donc pas prévue par la loi.

Conclusion : violation (6 voix contre 1).

Article 41 – La Cour a alloué une certaine somme pour frais et dépens. Le requérant n’a formulé aucune prétention au titre du dommage moral.

### Correspondance

Prévisibilité des écoutes téléphoniques effectuées dans le cadre d’une enquête préliminaire : violation.

***Arrêt PRADO BUGALLO c. Espagne (n° 58496/00). Arrêt 18.2 2003 [Section] :***

En fait : à la tête d’un vaste complexe économique composé de plusieurs sociétés d’import-export de tabac, le requérant disposait en Espagne d’un large réseau de collaborateurs. Dans le cadre d’une enquête judiciaire pour trafic de stupéfiants, sur demande du ministère de l’Intérieur, le juge d’instruction ordonna, par diverses ordonnances, la mise sur écoute de lignes téléphoniques de plusieurs personnes soupçonnées d’appartenir à un réseau de trafic de cocaïne dirigé par le requérant. Au terme des investigations policières, le requérant et plusieurs de ses collaborateurs furent arrêtés par la police et renvoyés en jugement pour plusieurs délits, dont trafic de stupéfiants et contrebande. Le requérant sollicita la nullité des preuves obtenues à la suite des écoutes téléphoniques. Le tribunal estima que les écoutes téléphoniques effectuées par la police étaient pleinement valables et se fonda notamment sur les enregistrements desdites écoutes pour déclarer le requérant coupable des délits reprochés. Le requérant fut condamné à une peine d’emprisonnement et au paiement d’amendes. Le Tribunal suprême confirma le jugement entrepris. Se référant à la jurisprudence de la Cour européenne des droits de l’homme, il estima que l’ingérence était justifiée eu égard à la gravité du délit de trafic de stupéfiants à grande échelle, et qu’elle était légale. Le requérant forma sans succès un recours d’amparo.

En droit : article 8 – Les garanties introduites par la loi organique 4/1988 du 25 mai 1988 précisant les modalités de contrôle de la mise sur écoute des conversations téléphoniques ne répondent pas à toutes les conditions exigées par la jurisprudence de la Cour pour éviter les abus. La loi s’avère insuffisante à cet égard, s’agissant en particulier des infractions pouvant donner lieu aux écoutes et de la fixation d’une limite à la durée d’exécution de la mesure. Les juridictions supérieures espagnoles ont estimé que les modifications opérées par cette loi étaient insuffisantes pour répondre aux garanties devant entourer les mises sur écoute téléphonique et ont jugé nécessaire de définir toute une série de garanties complémentaires. Aussi, si la loi de 1988 a apporté d’indéniables progrès, d’importantes lacunes persistaient au moment où les écoutes furent réalisées dans la présente affaire. Il est vrai que ces insuffisances ont été palliées en grande partie par la jurisprudence nationale. Cela étant, cette évolution jurisprudentielle, à supposer même qu’elle puisse combler les lacunes de la loi au sens formel, est intervenue après les ordonnances du juge d’instruction

décrétant la mise sur écoute des téléphones de personnes participant à l'activité délictueuse dirigée par le requérant. Dès lors, elle ne peut entrer en ligne de compte dans la présente affaire.

Conclusion : violation (unanimité).

Article 41 – La Cour alloue au requérant la somme de 7000 euros pour frais et dépens.

## Jurisprudence française

### Cour de cassation – Chambre criminelle

#### **Écoute des communications d'un avocat (arrêts des 21 mai et 1<sup>er</sup> octobre 2003)**

La jurisprudence de la chambre criminelle de la Cour de cassation a été riche en 2003 à propos des écoutes téléphoniques, spécialement sur la question de la légalité de l'écoute des communications d'un avocat. On sait en effet que la règle de libre communication entre la personne mise en examen et son avocat interdit l'interception de correspondances ou communications téléphoniques échangées entre eux. Toutefois, on savait que cette règle ne faisait pas obstacle à l'interception des communications d'un proche de cette personne avec l'avocat de celle-ci (crim. 10 mai 1994 : *Bull. crim.* n° 180).

On savait également que le juge d'instruction pouvait ordonner la captation et la transcription des conversations téléphoniques d'un avocat et de son client, dès lors que le contenu des conversations transcrites était de nature à contribuer à la manifestation de la vérité sur la participation de l'avocat aux infractions qui lui étaient reprochées et que les droits de la défense n'étaient pas en cause. Deux arrêts, respectivement de mai et octobre 2003, sont venus encore préciser – restreindre diront certains – le champ de la protection accordée au défenseur. Le premier arrêt (crim. 21 mai 2003) rappelle liminairement le principe dégagé par l'arrêt du 10 mai 1994, à savoir que la conversation entre un avocat et son client ne peut être transcrite et versée au dossier de la procédure que s'il apparaît que son contenu et sa nature sont propres à faire présumer la participation de l'avocat à une infraction. Ensuite, pour rejeter l'irrégularité alléguée des interceptions de communications, la chambre criminelle énonce que les avocats dont les conversations ont été transcrites n'avaient pas encore été désignés dans le dossier et que la mise en examen postérieure de X. ne reposant pas sur le contenu de ces conversations, il n'avait subi aucun grief (crim. 21 mai 2003).

Le deuxième arrêt (crim. 1<sup>er</sup> octobre 2003), s'il rappelle le principe de confidentialité des conversations entre une personne mise en examen et

son avocat, c'est pour énoncer que celui-ci ne saurait s'opposer à la transcription de certaines d'entre elles, dès lors qu'il est établi que leur contenu est de nature à faire présumer la participation de cet avocat à des faits constitutifs d'une infraction, fussent-ils étrangers à la saisine du juge d'instruction.

**Éléments constitutifs du délit d'appels malveillants  
(arrêt du 4 mars 2003)**

Le délit prévu à l'art. 222-16 C. pén. est caractérisé par des appels téléphoniques malveillants réitérés en vue de troubler la tranquillité d'autrui.

Méconnaît ce texte et ce principe la cour d'appel qui retient que la seule interlocutrice identifiée et entendue par les enquêteurs n'a reçu que deux communications téléphoniques dont la seconde suivait et complétait la première, ce qui excluait la réitération, ajoute que la teneur de la communication portant sur des faits de viol sur enfant handicapé était seulement susceptible d'éveiller l'attention de la correspondante ainsi portée à dénoncer ces agissements sans la perturber personnellement et en déduit que le caractère malveillant de l'appel n'est ainsi pas établi et que son but ou son résultat n'a pas été de troubler la tranquillité de la correspondante concernée, mais de l'inciter à en révéler le contenu afin de déclencher une enquête policière, alors que deux appels successifs, même effectués à des destinataires différents, suffisent à caractériser la réitération, la cour ne recherchant pas si l'intention de troubler la tranquillité d'autrui et le caractère malveillant des appels téléphoniques ne se déduisaient pas du contenu même du message.

**Tribunal de grande instance de Paris**

***Ordonnance de référé du 27 janvier 2003 :***

Après avoir entendu les parties comparantes ou leur conseil ;

Vu l'assignation en date du 20 janvier 2003 par laquelle D. expose qu'une personne se présentant comme M., *via* une boîte mail Lycos :...@lycos.fr, a adressé un message e-mail à trois de ses collaborateurs et un client important de la société – dont il est président de directoire – dont le contenu lui paraît diffamatoire ; demande au visa de l'article 145 du NCPC la communication par la société Lycos de l'identité de l'utilisateur de l'adresse électronique précitée et de conserver les mails envoyés depuis l'adresse ;

Vu les conclusions déposées à l'audience par la société Lycos qui fait valoir que le caractère privé de la correspondance incriminée s'oppose à ce qu'il soit fait droit à la demande et se déclare prête toutefois à communiquer l'identité qui lui a été déclarée par l'utilisateur de l'adresse électronique en cause ;

Attendu que les courriers électroniques sont des correspondances privées bénéficiant du secret, que dès lors, l'article 43-9 de la loi du 30 septembre 1986 modifiée n'est pas applicable à la demande de communication de l'identité du titulaire de l'adresse électronique :... @lycos.fr ;

que le même secret s'oppose à ce que la défenderesse puisse intercepter des messages enregistrés sous cette adresse, à supposer qu'ils n'aient pas été détruits, en les transférant sur un autre support en violation de l'article 226-15 du Code pénal ;

que la demande doit être rejetée ;

La décision

Statuant publiquement en premier ressort, par ordonnance contradictoire, Rejetons la demande ;

Laissons les dépens à la charge de D.

### **Tribunal de grande instance de Paris – 17<sup>e</sup> chambre**

#### ***Jugement du 28 février 2003 :***

[...] Attendu, d'autre part, que l'article 432-9 alinéa du Code pénal punit 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, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu ;

Attendu que le Conseil des marchés financiers est une autorité professionnelle investie d'une mission de service public, dès lors qu'elle est chargée d'exercer une fonction dont la finalité est de satisfaire à un intérêt général ; que ses inspecteurs ont agi en l'espèce dans le cadre de leurs attributions professionnelles ; qu'ils ont utilisé les correspondances émises par la voie des télécommunications, leur transmission au service de l'inspection du conseil des marchés financiers, qui fait partie de cet organisme, ne pouvant toutefois s'analyser en une divulgation au sens de l'article 432-9 du Code pénal ;

Attendu, cependant, que les prévenus ne sont pas passibles des sanctions prévues par ce texte s'ils justifient leur conduite par une permission de la loi ; que l'article susvisé précise expressément que l'interception ou le détournement de ces correspondances, l'utilisation ou la divulgation de leur contenu ne sont punissables que s'ils ont été commis « hors les cas prévus par la loi » ;

Or, attendu que le conseil des marchés financiers a été chargé, aux termes de l'article 67 de la loi du 2 juillet 1996 de modernisation des activités financières, de veiller au respect par les prestataires de services d'investissement des obligations professionnelles auxquelles ils sont astreints en

vertu de cette loi et du règlement général du conseil des marchés financiers, ce texte ayant par la suite été codifié à l'article L. 622-9-I du Code monétaire et financier ;

Attendu qu'en application de l'article 7-1-16 du règlement général du conseil des marchés financiers, « les personnes chargées du contrôle peuvent se faire communiquer tous documents qu'elles estiment utiles à leur mission, quel qu'en soit le support, et en obtenir copie » ;

Attendu que cet article laisse aux contrôleurs l'appréciation de l'utilité de ces documents ; que, dès lors que les conversations téléphoniques litigieuses ont été régulièrement enregistrées sur des lignes professionnelles au su des personnes concernées, les inspecteurs du conseil des marchés financiers étaient autorisés par ces textes légaux et réglementaires à en obtenir copie et à les utiliser, d'autant qu'il est, à juste titre, fait valoir en défense que les conversations incriminées ont été échangées entre les professionnels, que celle du 3 janvier 2001 avec Q. ne portait pas seulement sur la santé, les vacances et la gastronomie, mais aussi sur des sujets strictement professionnels, et que celle du 15 mai 2001 avec N. était relative à la réservation d'un restaurant un samedi, ce qui pouvait contribuer à établir les relations existant entre les interlocuteurs ;

Attendu, en conséquence, que le délit prévu par l'article 432-9 du Code pénal n'est pas constitué à l'encontre des prévenus ;

Par ces motifs

Le tribunal statuant publiquement, en matière correctionnelle, en premier ressort et par jugement contradictoire ;

Constate l'extinction de l'action publique par l'effet du désistement de la partie civile du chef de recel d'atteinte au secret des correspondances commise par des personnes chargées d'une mission de service public ;

RELAXE R. et S. du chef d'atteinte au secret des correspondances par une personne chargée d'une mission de service public et M. de complicité de ce délit.

## **Conseil d'État**

**Référé du 2 mai 2003, n° 255597, M. Germain G. :**

*Eu égard tant à la stricte réglementation par le Code de procédure pénale, et notamment par son article D. 417, des conditions dans lesquelles les détenus peuvent être autorisés à téléphoner, que des contraintes inhérentes à la sécurité dans les établissements pénitentiaires, aucune illégalité grave et manifeste ne ressort de la mesure par laquelle l'administration pénitentiaire a retiré à un détenu son téléphone cellulaire.*

[...] Vu la requête, enregistrée le 31 mars 2003 au secrétariat du contentieux du Conseil d'État, présentée par M. Germain G. ; M. G. demande au juge

des référés du Conseil d'État d'ordonner, sur le fondement de l'article L. 521-2 du Code de justice administrative, à l'administration pénitentiaire de lui restituer son téléphone cellulaire et de condamner l'État à lui verser une indemnité, au moins égale à 10 000 euros, en réparation du préjudice que la confiscation de ce téléphone lui a causé ;

Il soutient que l'administration pénitentiaire a porté une atteinte grave et manifestement illégale à son droit de propriété ;

Vu le code de justice administrative ;

Considérant qu'en égard tant à la stricte réglementation par le Code de procédure pénale, et notamment par son article D. 417, des conditions dans lesquelles les détenus peuvent être autorisés à téléphoner, que des contraintes inhérentes à la sécurité dans les établissements pénitentiaires, aucune illégalité grave et manifeste ne ressort, en l'état de l'instruction, de la mesure par laquelle l'administration pénitentiaire a retiré à M. G. son téléphone cellulaire ; qu'en outre il n'appartient pas au juge des référés d'allouer des indemnités ; qu'il est ainsi manifeste que la requête de M. G. est mal fondée ; que cette requête doit, dès lors, être rejetée selon la procédure prévue par l'article L. 522-3 du Code de justice administrative ;

ORDONNE :

Article 1<sup>er</sup> : la requête de M. Germain G. est rejetée ;

Article 2 : la présente ordonnance sera notifiée à M. Germain G. ;

Copie pour information en sera également transmise au garde des Sceaux, ministre de la Justice.

## Questions parlementaires

### **Opérateurs des télécommunications et sécurité – listes de données circulant sur internet à enregistrer par les opérateurs techniques**

**02956** – M<sup>me</sup> Nicole Borvo attire l'attention de M. le garde des Sceaux, ministre de la Justice, sur la question de la surveillance des données de communication publique et privée circulant sur l'internet, et de la définition des données devant donner lieu à l'enregistrement par les opérateurs techniques. La loi n° 2001-1062 du 15 novembre 2001, relative à la sécurité quotidienne introduit en effet, par son article 29, la nécessité pour les opérateurs de conserver un ensemble de données techniques, susceptibles d'être extraites à des fins d'enquêtes judiciaires. La nature exacte de ces données techniques, susceptibles d'être extraites à des fins d'enquêtes judiciaires. La nature exacte de ces données n'est certes pas encore connue, un décret en Conseil d'État devant compléter le texte de loi. Il n'en reste pas moins que les préconisations du G 8 et d'Europol en la matière sont de nature à inquiéter tant les prestataires techniques concernés que l'ensemble des citoyens français, tant elles vont à l'encontre du respect des libertés individuelles et des préceptes énoncés dans la déclaration universelle des droits de l'homme et du citoyen. En effet, que ce soit par son article 12, qui affirme le droit de chacun à la protection de sa vie privée et au secret de sa correspondance, ou son article 18, qui fonde le droit de tout individu à l'expression publique ou privée de ses opinions, cette déclaration est là pour nous rappeler combien il serait dommageable pour une démocratie de chercher à contrôler ou à restreindre par des mesures de surveillance systématique la libre circulation de l'information sur les réseaux de communication. Les mesures de vigilance que les citoyens français sont en droit d'attendre de l'État en matière de lutte contre le terrorisme ne sauraient en retour les faire considérer tous comme suspects par défaut et entraîner la mise en œuvre de

dispositifs d'écoute généraliste de l'ensemble du pays. La réflexion concernant les données que la justice peut légitimement demander aux opérateurs de conserver ne saurait être engagée sans consultation préalable de ceux que ces nouvelles mesures législatives vont concerner. Le législateur ne saurait faire l'impasse sur l'avis en la matière des opérateurs internet, mais pas plus sur celui des représentants de la société civile informatique, et plus largement de tous les utilisateurs des réseaux électroniques et de communication. Le droit imprescriptible à l'anonymat et à la vie privée ne saurait être diminué par de nouvelles lois d'exception prenant prétexte de nouveaux médias. Il existe déjà en France des dispositifs réglementaires sur la protection de la correspondance postale, sur l'informatique et les libertés, la protection des personnes et de leur vie privée, sur les propos racistes et antisémites. Reste à dégager, pour la justice et ses auxiliaires, les moyens, y compris sur internet, de la mise en œuvre de ces différentes lois. Elle lui demande donc quelles sont les intentions du gouvernement quant à la procédure d'établissement de la liste des données qui seront incluses dans le décret précisant la loi relative à la sécurité quotidienne. Elle lui demande également de surseoir à la rédaction de ce décret, pour permettre la mise en place d'une commission de travail compétente sur l'opportunité de conservation de chaque type de données, associant tous les acteurs concernés et aboutissant à la production d'un document qui ne soit pas que l'expression d'une angoisse exacerbée par la violence extrême d'actes isolés.

**Réponse** – Le garde des Sceaux, ministre de la Justice, fait connaître à l'honorable parlementaire qu'il ne partage pas les craintes que celle-ci exprime quant à un caractère attentatoire aux libertés fondamentales du dispositif prévu par l'article 29 de la loi du 15 novembre 2001 relative à la sécurité quotidienne, lequel permet au gouvernement de prendre par voie réglementaire des mesures conduisant les opérateurs de télécommunications à conserver pendant une durée maximale d'un an certaines données techniques relatives aux communications, dites parfois « données de connexion ». En effet, ces mesures, dont le but exclusif est de permettre en tant que de besoin la mise à disposition de l'autorité judiciaire de telles ou telles de ces données, ne sauraient en aucun cas être assimilées, ainsi qu'il est suggéré par l'auteur de la question, à une surveillance systématique de l'information circulant sur les réseaux de communication, ou à un dispositif d'écoute généralisé de l'ensemble des citoyens français. Sur ce point, il est en effet clairement énoncé par la loi susvisée que les données ainsi conservées, si elles rendent possible l'identification de l'utilisateur d'un service de télécommunications, ne peuvent en revanche d'aucune manière porter, comme le ferait une interception de correspondance émise par la voie des télécommunications, sur le contenu des correspondances échangées ou des informations consultées. Ces raisons expliquent que la conservation temporaire des données dites de connexion ne constitue pas à proprement parler une ingérence dans la liberté d'expression et de communication. Il doit du reste être observé que les dispositions suscitant les inquiétudes de l'honorable parlementaire sont en stricte conformité avec les possibilités expressément ménagées aux États dans un but de prévention, de

recherche, de détection et de poursuite d'infractions pénales, par l'article 15 de la directive du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. Par ailleurs, ces dispositions ne sont aucunement contraires aux principes énoncés dans la Déclaration universelle des droits de l'homme proclamée par l'Assemblée générale des Nations unies, le 10 décembre 1948. En effet, l'exercice des droits prévus aux articles 12 et 18 de celle-ci, lesquels prohibent les immixtions arbitraires dans la vie privée ou la correspondance et proclament le droit de toute personne à la liberté de pensée de conscience et de religion, ne peut se concevoir concrètement sans un certain nombre de limitations. L'édiction de celles-ci par la loi est expressément envisagée par l'article 29 de la Déclaration, et elle peut être autorisée notamment pour assurer la reconnaissance et le respect des droits et libertés d'autrui et la prise en considération des exigences de l'ordre public dans une société démocratique. À cet égard, dans un contexte marqué par les menaces terroristes que doivent affronter les sociétés démocratiques contemporaines, le gouvernement ne peut faire sienne l'opinion selon laquelle les libertés dont il convient d'assurer le respect sur les réseaux électroniques de communication se traduisent par « un droit imprescriptible à l'anonymat ». Une telle analyse conduirait en effet à paralyser la lutte contre de multiples activités terroristes et de nombreuses formes de délinquance organisée qui s'exercent par le biais des réseaux de communication électronique. S'agissant enfin des aspects de la présente question qui concernent les modalités d'élaboration du décret d'application de l'article 29 de la loi susvisée du 15 novembre 2001, il importe de préciser que la procédure qui devra être suivie à cet égard de par un choix du législateur, prévoit un haut niveau de garanties, puisque ce texte réglementaire requiert la double consultation de la Commission nationale de l'informatique et des libertés et du Conseil d'État. Il convient par ailleurs de rappeler que les dispositions qui figurent à l'article 29 de la loi sur la sécurité quotidienne ont d'ores et déjà fait l'objet d'une consultation publique dans le cadre de l'élaboration du projet de loi sur la société de l'information, où elles figuraient initialement. En outre, sous la présente législature, elles ont été soumises aux opérateurs de télécommunication. Dans ces conditions, il n'apparaît pas que de nouvelles mesures de concertation de la nature de celles proposées par l'honorable parlementaire soient nécessaires.

### **Télécommunications (téléphone – portables – centres de traitement de l'alerte – appels malveillants – neutralisation)**

**7928 – 9 décembre 2002** – M. Jean-François Mancel interroge M<sup>me</sup> la ministre déléguée à l'Industrie sur les mesures qu'elle envisage de prendre pour lutter contre l'accroissement exponentiel du nombre des appels malveillants reçus dans les centres de traitement de l'alerte. Le centre de traitement de l'alerte de l'Oise reçoit ainsi entre 800 et 1 500 appels malveillants par jour, ce qui risque de provoquer une saturation du standard

téléphonique. Les auteurs de ces appels utilisent pour ce faire des téléphones cellulaires dont la carte d'identification (SIM) a été neutralisée, ce qui ne permet pas leur identification. Contrairement à ce que le secrétaire d'État à l'Industrie avait indiqué le 7 août 2000 suite à une question n° 42-220 posée par Hervé Gaymard, député de la Savoie, aucun numéro de série du terminal utilisé ne s'affiche sur les écrans du CTA. Il lui demande par conséquent s'il est techniquement possible d'équiper les téléphones portables d'un deuxième dispositif d'identification inamovible, paramétrable par les seuls opérateurs de téléphonie mobile et spécialement dédié aux numéros d'appel d'urgence : un appareil volé ne doit plus pouvoir être utilisable, y compris lorsque c'est le 112 qui est composé. Il souhaite également savoir s'il existe un moyen simple et rapide pour les opérateurs du CTA de retrouver l'identité et la localisation de l'appelant à partir de son numéro de téléphone, lorsque celui-ci s'affiche. Enfin, il suggère de ne plus associer, dans les notices d'utilisation des appareils portables, l'abréviation « SOS » au numéro 112 : certains abonnés sont en effet persuadés que, lorsqu'ils composent le 112, ils sont mis en relation avec un service d'assistance pour l'utilisation de leur terminal.

**Réponse** – L'autorisation administrative délivrée aux opérateurs de téléphonie mobile d'exploiter un réseau de télécommunications ouvert au public en application des dispositions de l'article L. 33-1 du Code des postes et télécommunications fixe leurs obligations. Le cahier des charges annexé à l'arrêté d'autorisation précise que les opérateurs 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. Concernant les appels émis à partir de terminaux dont la carte « SIM » a été retirée ou invalidée, l'état actuel de la technique et la configuration des réseaux des opérateurs ne permettent pas de prendre une mesure telle que celle envisagée par l'honorable parlementaire. Toutefois, dans le cadre de la loi pour la sécurité intérieure, il est prévu la mise en œuvre, par les opérateurs, d'une base de données relative à l'identité des terminaux volés et notamment de leurs numéros « IMEI » (International Mobile Equipment Identity), ce qui doit permettre d'empêcher l'utilisation de ces téléphones et pas seulement de bloquer les cartes SIM. Cette disposition, en cours de mise en œuvre, réduira beaucoup les possibilités d'utiliser des téléphones mobiles volés, y compris pour passer des appels à destination du 112. Concernant la possibilité pour le centre de traitement de l'alerte (CTA) de retrouver l'identité et de localiser l'appelant, il convient de signaler que, dans le cadre de la loi pour la sécurité intérieure, les services d'urgence pourront bénéficier de modalités d'accès simplifiées à la liste rouge.

## **Télécommunications (internet – cybercriminalité – lutte et prévention)**

**14140 – 17 mars 2003** – M. Claude Goasguen attire l'attention de M. le ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales sur la lutte contre la délinquance pédophile sur internet. Face à une croissance alarmante du trafic pédophile sur internet, il apparaît que les moyens mis à la disposition des enquêteurs de la justice sont de plus en plus dérisoires au fur et à mesure que se développent les échanges et que les techniques informatiques se perfectionnent. Il faut souvent analyser des milliers de messages, décoder des centaines d'adresses électroniques, de codes informatiques, pour constituer des preuves de la culpabilité des pédophiles utilisant le réseau pour sévir. Ce travail demande à la fois du temps, des compétences particulières et du matériel informatique adapté. Si la compétence des équipes qui traquent inlassablement ces criminels n'est pas remise en cause, les connaissances techniques nécessaires demandent une formation spécifique qui n'est pas toujours prévue pour les enquêteurs ; de plus, les moyens dont ils disposent sont malheureusement mal adaptés à ce type de délinquance, alors que souvent deux ans s'écoulent avant que des résultats tangibles ne permettent au procureur de la République, par exemple, de poursuivre son action suite à des plaintes. Les conséquences de cette lenteur technique d'investigation peuvent être cependant douloureuses, puisque certains pédophiles, arrêtés après leur méfait, apparaissent plus tard comme appartenant à un réseau en ligne. Il voudrait connaître ses intentions pour accroître l'efficacité de la lutte contre les pédophiles sévisant sur internet.

**Réponse** – La lutte contre les actes délictuels et criminels de toute nature commis sur l'internet, et parmi eux les actes à caractère pédophile, a toujours constitué une priorité pour les services du ministère de l'Intérieur. Dans sa lutte contre la délinquance, contre la criminalité sur internet et contre les actes à caractère pédophile commis sur internet, la direction centrale de la police judiciaire (DCPJ) dispose d'un ensemble d'outils répressifs et de structures appropriées qui témoignent de sa réactivité et de son adaptation aux phénomènes criminels nouveaux. Au niveau des structures, la création au mois de septembre 1997, au sein de la sous-direction des affaires criminelles (SDAC), d'un groupe spécialisé chargé des mineurs victimes, appartenant à la division nationale pour la répression des atteintes aux personnes et aux biens (DNRAPB), a répondu à l'impératif de mise en place d'une entité spécialisée au sein de la DCPJ. Ce groupe a été investi de deux missions prioritaires, une mission opérationnelle d'enquêtes judiciaires et une mission de centralisation de la documentation opérationnelle. L'exploitation de cette documentation a confirmé la nécessité de répertorier et de traiter en priorité les images pornographiques mettant en scène des mineurs afin d'identifier les victimes et les auteurs et d'établir les liens entre les différentes affaires. Les services de police européens estiment entre 600 000 et 700 000 le nombre d'images pornographiques mettant en scène les mineurs circulant sur le réseau internet à travers le monde. En raison de

la technicité des investigations concernant des infractions utilisant internet comme vecteur, ce groupe peut s'appuyer sur l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), créé en mai 2000, au sein duquel une unité a tout spécialement été mise en place pour procéder à la surveillance et au suivi des sites internet susceptibles de stocker et de diffuser des images pornographiques impliquant des mineurs. Cette unité agit comme une cellule de veille policière permanente sur le réseau mondial. Le domaine de compétence de l'office est fixé par l'article 2 du décret précité : sont du ressort de l'OCLCTIC les infractions spécifiques à la criminalité liée aux technologies de l'information et de la communication et les infractions dont la commission est facilitée ou liée à l'utilisation de ces technologies. L'office anime et coordonne au plan national la mise en œuvre opérationnelle de la lutte contre les auteurs d'infractions spécifiques à la criminalité liée aux technologies de l'information et de la communication, procède à la demande de l'autorité judiciaire, à tous actes d'enquêtes et de travaux techniques d'investigations en assistance aux services chargés d'enquêtes de police judiciaire sur ces infractions, apporte une assistance aux services de police, de gendarmerie, de la douane, de la direction générale de la concurrence, de la consommation et de la répression des fraudes en cas d'infractions liées aux technologies de l'information et de la communication et d'intervenir d'initiative, avec l'accord de l'autorité judiciaire saisie, pour s'informer sur place des faits relatifs aux investigations conduites. L'OCLCTIC a également créé et assure le suivi de l'adresse électronique [www.internet-mineurs.gouv.fr](http://www.internet-mineurs.gouv.fr), sur laquelle les internautes peuvent adresser toute dénonciation concernant des sites accueillant des images pornographiques impliquant des mineurs. Une enquête est alors diligentée d'initiative et les faits dénoncés au parquet. Les éléments ainsi recueillis dans une base de données sont, si le contenu est effectivement illégal, exploités techniquement par l'OCLCTIC. Cette exploitation technique consiste en la localisation géographique du serveur diffusant le contenu illicite et l'identification du propriétaire du nom de domaine, lorsqu'il s'agit d'un site web. Les informations recueillies sont transmises au parquet territorialement compétent (implantation du serveur et/ou domiciliation du titulaire du nom de domaine) qui fait diligenter une enquête par les services de police spécialisés dans la protection des mineurs. Si le serveur est situé à l'étranger, les informations techniques sont transmises aux autorités locales par le canal d'Interpol. S'agissant de sites diffusant d'autres contenus illicites (haine raciale, apologie de crimes...), l'OCLCTIC ne dispose pas de compétences d'attribution particulières. Il apporte son assistance technique au service de police initialement saisi ou relaie l'information aux services concernés, si celle-ci lui parvient directement (par messagerie électronique, par exemple). L'action de ces deux services centraux à compétence nationale et internationale est relayée au niveau territorial par les services régionaux de police judiciaire (SRPJ) et par la brigade de protection des mineurs de la direction régionale de police judiciaire de Paris (DRPJ), qui bénéficient également de l'appui de ces deux services spécialisés lorsque la technicité ou l'ampleur des investigations l'exige. Chaque SRPJ

est à même de lutter contre ces infractions, tant au point de vue procédural que technique, avec l'apport des enquêteurs spécialisés en criminalité informatique qui sont les correspondants de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication au sein duquel un groupe est spécialisé dans la surveillance et le suivi des sites « internet » susceptibles de stocker et de diffuser des images pornographiques impliquant des mineurs et qui procède aux premières investigations sur les dénonciations faites par les internautes sur l'adresse électronique [www.internet-mineurs.gouv.fr](http://www.internet-mineurs.gouv.fr). Au plan international, la DCPJ a poursuivi ses efforts au plus près des avancées technologiques. En effet, si plusieurs pays européens disposent d'une « bibliothèque » de supports pornographiques constituée au gré des saisies judiciaires et si l'organisation internationale de police criminelle – Interpol – a annoncé sa décision de se doter d'une base de données d'images pédophiles avec accès sécurisé à l'usage exclusif des services de police, il n'existe cependant pas de système de centralisation capable de traiter la masse des données. Un tel système permettrait de réaliser des recoupements nationaux ou internationaux concernant des photographies liées à un même réseau. Dans le cadre du programme de financement européen « STOP » (Sexual Trafficking of Persons), la DCPJ a entrepris de développer un logiciel d'indexation et de recherche automatique par le contenu de l'image qui a abouti à la création du logiciel « Image seeker », acheté par Interpol et les douanes américaines. Cet outil informatique peut être configuré selon les diverses recommandations du « G8 ». Une norme internationale d'indexation est en cours d'étude à l'OIPC/Interpol avec la participation active de la direction centrale de la police judiciaire. La première phase conduite en 1999 a permis de faire développer par l'Institut national de la recherche informatique et automatisme (INRIA) un prototype novateur issu des dernières technologies en matière de comparaison d'images. La deuxième phase, en cours aujourd'hui, prévoit les travaux de programmation spécifiquement adaptés aux besoins particuliers des services de police et les tests actuellement menés en partenariat avec des policiers espagnols. Cet outil informatique permettra une indexation automatique de l'ensemble des supports pornographiques impliquant des mineurs (disque compact, film, disquette informatique, photographie, vidéographie, etc.), une recherche automatique en temps réel à partir d'une image requête saisie lors d'une opération judiciaire, fonctionnalité qui pourra être affinée par une recherche spécifique sur les visages et une requête partielle à partir d'un objet contenu dans l'image. Ce système, dont la finalisation technique devrait intervenir avant l'été, permettra le traitement rapide d'un nombre illimité d'images, notamment à partir des nouveaux supports informatiques (cédéroms, DVD...) et de pallier ainsi les difficultés rencontrées lors des enquêtes concernant des pédophiles ayant utilisé internet. Au niveau juridique, le travail des enquêteurs s'est vu conforté par plusieurs dispositions législatives : la loi du 17 juin 1998 a permis de procéder à une refonte générale des instruments de prévention et de répression des infractions de nature sexuelle ou de celles commises contre des mineurs. Ce texte a notablement aggravé la répression des infractions

de nature sexuelle, spécialement lorsque celles-ci sont commises à l'encontre des mineurs. Par ailleurs, l'importation et l'exportation de documents pornographiques mettant en scène des mineurs, y compris lorsque les documents ne font que transiter par le territoire français pour être ensuite réexpédiés vers des pays tiers, sont désormais incriminées spécifiquement. Enfin, l'utilisation des réseaux de télécommunication, et notamment du réseau internet, pour commettre une infraction à caractère sexuel a été prise en compte et érigée en circonstance aggravante. L'article 29 de la loi de 2001 relative à la sécurité quotidienne fait obligation aux opérateurs de télécommunication pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales de différer pour une durée maximale d'un an les « opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques ». Cette mesure doit permettre à la justice d'avoir accès à l'identification des personnes ayant utilisé le réseau internet pour charger des supports pornographiques impliquant des mineurs. Cette disposition a été pérennisée par la loi du 18 mars 2003 pour la sécurité intérieure qui autorise désormais les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire à accéder, au cours d'une perquisition, par un système informatique implanté sur les lieux où se déroule l'opération, à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial. Cet arsenal préventif et répressif a déjà permis de démanteler plusieurs réseaux d'alimentation d'internet en images pornographiques impliquant des mineurs. Les affaires les plus récentes soulignent l'engagement fort de l'ensemble des services de la DCPJ dans des affaires qui ont très souvent un caractère international. Les 13 et 18 mars 2002, exploitant un *listing* transmis par Interpol, les enquêteurs du service régional de police judiciaire d'Angers, avec l'apport des enquêteurs spécialisés de l'OCLTIC, interpellaient deux enseignants sur les ordinateurs desquels étaient retrouvées plusieurs centaines de milliers de photographies pornographiques impliquant des mineurs. Le 13 mars 2002, coopérant avec leurs collègues de la police criminelle fédérale allemande, les enquêteurs de la direction centrale de la police judiciaire et du SRPJ de Strasbourg interpellaient à Rohrbach-lès-Bitche (57) un homme dans l'ordinateur duquel les fonctionnaires de l'OCLTIC découvraient plusieurs milliers de photographies pornographiques de mineurs dont certains de sa famille qu'il diffusait sur internet. Le 16 avril 2002, sur la base d'un autre renseignement émanant des autorités allemandes, la DCPJ (DNRAPB, l'OCLTIC et le SRPJ) déclenchait une opération d'envergure nationale. L'enquête conduisait à l'interpellation de 35 internautes à travers la France. Plusieurs centaines de milliers d'images ou vidéogrammes pornographiques impliquant des mineurs étaient retrouvés. Quelques images mettaient en scène certains internautes interpellés. Le 12 février 2003, les enquêteurs de la DCPJ interpellaient à Marseille un homme qui s'était vanté sur internet, lors de « chats » (forum de discussions) avec un internaute précédemment interpellé par la DNRAPB, d'avoir filmé les agressions sexuelles auxquelles il s'était livré sur sa fille

âgée de six ans. Au cours de la perquisition, les enquêteurs découvraient sur l'ordinateur du mis en cause les films incriminés. Une seconde victime, amie de la famille, âgée de neuf ans, apparaissait également dénudée sur les images saisies. Les auditions permettaient d'apprendre que la fille du mis en cause pourrait avoir été droguée par ingestion de médicaments avant de subir les viols. À l'issue de sa garde à vue, il était placé sous mandat de dépôt. Dans le cadre d'une enquête conjointe avec les polices cantonales de Berne et Genève, les enquêteurs de la DNRAPB identifiaient un groupe d'internautes échangeant des images à caractère pornographique impliquant des mineurs sur le réseau internet. Huit personnes étaient identifiées et interpellées le 9 décembre 2002 sur le territoire national. Plusieurs centaines de milliers d'images pornographiques impliquant des mineurs étaient saisies chez l'ensemble des mis en cause. La poursuite des investigations permettait de confondre l'un des mis en cause comme étant l'auteur de sévices sexuels et de viol sur son neveu de trois ans. Au plan international seize arrestations ont été opérées au Canada, en Belgique, en Grande-Bretagne et en Suisse. Les policiers canadiens ont pu élucider le viol de deux enfants de trois ans par l'un des mis en cause.

### **Système pénitentiaire (évasions – lutte et prévention – téléphones portables)**

**15023 – 24 mars 2003** – M. Jean-Marc Roubaud appelle l'attention de M. le garde des Sceaux, ministre de la Justice, sur la situation des prisons françaises. Que ce soit à Borgo ou à Fresnes, les deux dernières évasions de nos prisons ont profondément choqué les Français, comme le personnel pénitentiaire. Même si le nombre global des évasions en France est passé de trente-quatre en 2000 à quinze en 2002, il n'en demeure pas moins que nos concitoyens ont le sentiment d'un grand malaise face à ces évasions. En conséquence, il demande s'il entend prendre des mesures particulières ou créer des structures spécifiques pour la détention des individus les plus dangereux.

**Réponse** – Le garde des Sceaux, ministre de la Justice, porte à la connaissance de l'honorable parlementaire que la sécurité des établissements pénitentiaires constitue une priorité de l'action gouvernementale. Par arrêté du garde des Sceaux, ministre de la Justice, en date du 9 janvier 2003, un département de l'état-major de sécurité a été créé au sein de la direction de l'administration pénitentiaire, comprenant trois bureaux (gestion de la détention, sécurité pénitentiaire, renseignement pénitentiaire). Par ailleurs, des mesures concrètes ont été sans attendre décidées : mise en place d'un dispositif d'aide à la visée pour les agents armés affectés en miradors, renforcement des contrôles aux parloirs (notamment par l'introduction de techniques biométriques d'identification afin d'éviter les évasions par substitution), port de gilets pare-balles pour les personnels lors de missions au cours desquelles des risques particulièrement élevés sont encourus, renforcement de la sécurité périmétrique des établissements les plus sensibles. Des audits de sécurité sont régulièrement menés par la brigade

de sécurité pénitentiaire (BSP) à la demande de cet état-major. Par ailleurs, la loi d'orientation et de programmation pour la justice (LOPJ) a fixé six priorités pour les cinq années à venir : la sécurisation des maisons centrales (5 millions d'euros) ; l'installation de filins antihélicoptères et la pose de dispositifs « d'antiescalade » sur les toitures (2,63 millions d'euros) ; l'équipement des établissements en téléphonie sans fil ou radiocommunications, associé à un système d'alarme (20 millions d'euros) ; l'installation de tunnels d'inspection à rayons X (5 millions d'euros) ; le brouillage des téléphones portables (25 millions d'euros). Certains quartiers d'établissements sensibles sont d'ores et déjà équipés d'appareils de brouillage. Ce programme de sécurisation des établissements, sans précédent, se traduit également par la mise en place d'équipes régionales d'intervention et de sécurité (ERIS). Ces ERIS, créées par circulaire du garde des Sceaux, en date du 27 février 2003, ont une triple vocation : renforcer les structures locales, participer à l'organisation de fouilles, rétablir l'ordre avant l'intervention éventuelle des forces de police ou de gendarmerie. Les ERIS seront opérationnelles en octobre 2003. Des événements récents qui se sont déroulés depuis le début de l'année ont démontré la présence en détention d'armes et de substances explosives. Le garde des Sceaux a décidé, dans ce contexte, de mettre en œuvre sans délai, une opération spéciale de fouille des établissements pénitentiaires les plus sensibles. Ce programme de fouille est actuellement en cours d'exécution. Il convient enfin de noter que la décision a été prise de créer deux nouvelles maisons centrales où pourront être affectés des détenus particulièrement dangereux.

### **Défense (télécommunications – communications satellitaires – perspectives)**

**17979 – 12 mai 2003** – Un des enseignements tirés des opérations militaires en Afghanistan est que les talibans s'appuyaient sur des communications satellitaires, plus difficiles à intercepter. Devant la menace que constituent des groupes terroristes bien équipés, M. Bruno Bourg-Broc demande à M<sup>me</sup> la ministre de la Défense quels sont les matériels qu'elle compte faire mettre en œuvre pour résoudre ce genre de problème.

**Réponse** – Les forces armées disposent déjà de moyens d'interception des communications relayées par satellite. Toutefois, pour faire face à l'évolution rapide des technologies et à l'utilisation croissante de ce type de communication, le ministère de la Défense s'est engagé dans une démarche de modernisation et d'augmentation de ses capacités dans ce domaine. La délégation générale pour l'armement mène au profit de la direction du renseignement militaire et de l'état-major de l'armée de terre une vaste opération de refonte des moyens de ces organismes en matière d'interception des communications satellitaires. Cette opération, dont le financement est prévu dans la loi de programmation militaire 2003-2008, a pour objectif de les doter à court terme de capacités importantes intégrant l'évolution des technologies des télécommunications.

## **Télécommunications (téléphone – portables – numéros – confidentialité)**

**22345 – 21 juillet 2003** – M. Jean Bardet appelle l'attention de M. le secrétaire d'État aux Petites et Moyennes Entreprises, au Commerce, à l'Artisanat, aux Professions libérales et à la Consommation sur le respect de la confidentialité des numéros de téléphone portable inscrits sur liste rouge par l'opérateur même. Le prestataire de service a, de par le contrat commercial, les coordonnées de tous ses abonnés. De ce fait, il peut profiter de cette situation pour appeler ses clients à des fins publicitaires et commerciales. Il a donc la capacité de ne pas respecter lui-même le service qu'il propose. Il lui demande donc de bien vouloir lui préciser si de tels actes sont permis par la loi.

**Réponse** – Le numéro d'un téléphone portable constitue une donnée à caractère personnel dont la collecte, le traitement et l'utilisation sont régis, d'une part, par les textes de portée générale que sont la loi n° 78-17 du 6 janvier 1978 relative à l'informatique et aux libertés et la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et, d'autre part, par des dispositions sectorielles que sont les articles L. 33-4 et R. 10 et suivants du Code des postes et télécommunications (CPT) relatifs aux annuaires universels et les articles L. 33-4-1 du CPT et L. 121-20-5 du Code de la consommation relatifs aux communications non sollicitées. Ces deux derniers articles vont être prochainement modifiés et complétés par le projet de loi pour la confiance dans l'économie numérique, examiné en première lecture par le Parlement et transposant, notamment, les dispositions de la directive 2002/58/CE relative à la vie privée et aux communications électroniques. L'inscription d'un numéro de téléphone en liste dite « rouge » correspond au droit des personnes à s'opposer à la publication de leurs coordonnées dans les annuaires d'abonnés, imprimés ou électroniques, accessibles au public ou consultables par l'intermédiaire de services de renseignements ou des services d'annuaires inversés et à leur revente à des services marketing. S'agissant de la faculté d'utilisation des coordonnées à des fins de prospection, celle-ci est strictement encadrée, qu'il s'agisse d'une prospection téléphonique classique avec intervention humaine ou d'une prospection par automate d'appel ou par SMS (*Short Message Service*). Le projet de loi pour la confiance dans l'économie numérique pose le principe de l'interdiction de prospection sans le consentement préalable de l'abonné. Ce texte étend au SMS ce régime dit d'*opt in* déjà en vigueur pour les automates d'appel. Il prévoit cependant, à titre dérogatoire, que les entreprises ayant, ou ayant eu, une relation contractuelle avec un client (ce qui est le cas de l'opérateur fournissant le service téléphonique) peuvent utiliser les coordonnées de ce dernier aux fins de prospection, si l'abonné a été informé de l'éventualité d'une telle utilisation et s'il se voit expressément offrir la possibilité de s'opposer, sans frais et de manière simple, à cette utilisation de ses coordonnées. L'article R. 10-4 du Code des postes et télécommunications, modifié par le décret 2003-752 du 1<sup>er</sup> août 2003, rappelle également cette

dérogation. En conclusion, un opérateur mobile peut prospecter ses abonnés par appel téléphonique classique et par SMS sous réserve, notamment, du respect des principes d'information et de droit d'opposition de la personne concernée. La prospection par automate d'appel n'est quant à elle autorisée qu'avec le consentement préalable de l'abonné.

### **Télécommunications (appels d'urgence – utilisation malveillante – lutte et prévention)**

**24534 – 15 septembre 2003** – M. Jean-Paul Bacquet attire l'attention de M. le ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales sur la recrudescence d'appels malveillants reçus par les centres de traitement des alertes des sapeurs-pompiers et les centres de réception et de régulation des appels des SAMU. Pour ce qui concerne les appels du 15 et du 18, le numéro de l'appelant est systématiquement acheminé par France Télécom sur des autocommutateurs permettant l'affichage du numéro de l'appelant, voire la récupération automatique de l'adresse de ce dernier. Cette mesure apporte un surcroît de sécurité notoire pour les malades qui n'ont pas la capacité de s'exprimer au téléphone et cela permet surtout au service d'urgence de retrouver les coordonnées des personnes malveillantes abusant du dispositif. Par contre, deux difficultés apparaissent, à savoir que le numéro européen des urgences, le 112, n'a pas bénéficié de la même facilité d'acheminement du numéro de l'appelant que le 15 et le 18. En particulier, le numéro de l'appelant ne s'affiche pas pour les appels arrivant du 112, dès lors que l'appelant a décidé de masquer son numéro. La sécurisation de l'appel n'est donc pas apportée et l'appel malveillant éventuel ne peut pas être identifié. L'usage des téléphones portables est venu encore aggraver cette difficulté dans la mesure où le titulaire du téléphone portable peut appeler le 112 avec son numéro masqué et, de plus, on peut appeler le 112 avec les téléphones portables dont la carte SIM a été retirée ou désactivée, donc pas d'identification. Pour le département du Puy-de-Dôme, dont la population est de 600 000 habitants, il a été dénombré plus de 30 000 faux appels par malveillance en 2002. Fin juillet 2003, le nombre atteint déjà les 20 000 appels (ces statistiques sont exclusivement celles du SAMU 63). Le harcèlement téléphonique des permanenciers des SAMU et des stationnaires du CODIS représente une réelle mise en danger de la population dans la mesure où ces appels malveillants mobilisent les ressources téléphoniques et la bande passante des lignes de France Télécom. Il est clair qu'il y a, dans ce cadre, mise en danger de la vie d'autrui. Au moment où les fournisseurs de téléphonie privée vont être amenés à mettre les numéros des abonnés du téléphone portable sur un annuaire et où le changement de fournisseur permettra la conservation du numéro d'abonné, il paraît particulièrement important qu'une réglementation, assurant à la fois la sécurité des usagers et la protection des centres de traitement des alertes des sapeurs-pompiers et les centres de réception et de régulation des appels contre les appels malveillants, soit mise en place de manière simultanée. Aussi, afin d'éviter ces appels malveillants qui ne cessent d'augmenter, il lui demande de lui

préciser les mesures qu'il entend mettre en place rapidement. – Question transmise à M. le ministre de la Santé, de la Famille et des Personnes handicapées.

**Réponse** – L'honorable parlementaire a attiré l'attention sur l'importante recrudescence des appels malveillants reçus par les centres de traitement de l'alerte des sapeurs-pompiers et les centres de réception et de régulation des appels du SAMU, à partir du numéro 112, au moyen de portables dépourvus de carte SIM ou dont la carte SIM a été désactivée. Dans ce cas, les appels ne sont pas identifiables et, à ce jour, 80 % des appels arrivant au SAMU par le 112 sont des appels malveillants. Lors de la séance de la commission interministérielle de coordination des réseaux et des services de télécommunications (CICREST) pour la défense et la sécurité publique du 4 juin 2003, M. Didier Lallemand, haut fonctionnaire de défense du ministère de l'Économie, des Finances et de l'Industrie, président de la CICREST, à la demande des ministères de la Santé, de l'Intérieur et de la Défense, a souhaité que les appels polluants émis à partir de téléphones portables sans carte SIM et reçus sur le 112 puissent être éliminés afin de permettre à tous les services d'urgence en charge de la gestion de ce numéro (SAMU, sapeurs-pompiers, police, gendarmerie) de mieux concentrer leur activité sur les appels au secours. L'ensemble des services d'urgence sont en effet confrontés à une croissance exponentielle des appels (multiplication par 12 entre 1997 et 2001) en lien direct avec le développement de la téléphonie mobile. Durant cette période, les appels polluants voire malveillants sur le 112 provenant essentiellement de portables sans carte SIM, ont représenté plus de 80 % du volume traité et n'ont pu être identifiés. Il en est de même des appels provenant de mobiles avec carte SIM, mais dont le code PIN n'a pas été activé. Actuellement les terminaux dépourvus de carte SIM ou ceux dont le code PIN n'a pas été activé n'ont accès ni au 15, ni au 18 ni au 17. L'interdiction de ce type d'appel constitue donc un enjeu essentiel pour les services d'urgence. L'absence de règlement de cette question mettrait en effet directement en cause la qualité et la célérité de la réponse des services publics aux appels au secours des citoyens. À cet égard, l'accès au 112 n'est pas autorisé pour les portables dépourvus de carte SIM en Espagne, en Belgique et au Royaume-Uni. Le ministère de la Santé, de la Famille et des Personnes handicapées souhaite donc que l'accès au 112 soit interdit aux mobiles dépourvus de carte SIM et aux mobiles dont le code PIN n'est pas activé.

# Table des matières

|                                                                            |    |
|----------------------------------------------------------------------------|----|
| <b>Sommaire</b> .....                                                      | 3  |
| <b>Avant-propos</b> .....                                                  | 5  |
| Première partie                                                            |    |
| <b>RAPPORT D'ACTIVITÉ</b> .....                                            | 7  |
| Chapitre I                                                                 |    |
| <b>Organisation et fonctionnement de la Commission</b> .....               | 9  |
| Composition de la Commission .....                                         | 9  |
| Rappel des compositions successives de la Commission .....                 | 10 |
| Financement .....                                                          | 11 |
| Fonctionnement .....                                                       | 11 |
| Chapitre II                                                                |    |
| <b>Le contrôle des autorisations</b> .....                                 | 13 |
| Les modalités du contrôle .....                                            | 13 |
| Données chiffrées et commentaires .....                                    | 16 |
| Tableaux annexes .....                                                     | 20 |
| Chapitre III                                                               |    |
| <b>Le contrôle de l'exécution</b> .....                                    | 25 |
| Enregistrement, transcription et durée des interceptions .....             | 25 |
| Le contrôle du GIC .....                                                   | 26 |
| Les visites sur le terrain .....                                           | 26 |
| Réclamations de particuliers et dénonciation à l'autorité judiciaire ..... | 27 |

---

Table des matières

|                                                                                                         |    |
|---------------------------------------------------------------------------------------------------------|----|
| Chapitre IV                                                                                             |    |
| <b>Le contrôle du matériel</b> . . . . .                                                                | 29 |
| Chapitre V                                                                                              |    |
| <b>Actualités de l'année 2003</b> . . . . .                                                             | 33 |
| Deuxième partie                                                                                         |    |
| <b>ÉTUDES ET DOCUMENTS</b> . . . . .                                                                    | 35 |
| Chapitre I                                                                                              |    |
| <b>Présentation ordonnée des textes relatifs aux interceptions</b> . . . . .                            | 37 |
| Les interceptions ordonnées par l'autorité judiciaire . . . . .                                         | 38 |
| Textes réglementaires récents visant la loi du 10 juillet 1991 . . . . .                                | 46 |
| Chapitre II                                                                                             |    |
| <b>Actualité législative</b> . . . . .                                                                  | 49 |
| Télécommunications . . . . .                                                                            | 49 |
| Procédure pénale . . . . .                                                                              | 49 |
| Chapitre III                                                                                            |    |
| <b>Réflexions sur le motif d'interception « sécurité nationale »</b> . . . . .                          | 53 |
| L'origine du concept . . . . .                                                                          | 53 |
| Le contenu du concept . . . . .                                                                         | 55 |
| Les observations de la Commission sur le motif d'interception<br>« sécurité nationale » . . . . .       | 57 |
| Chapitre IV                                                                                             |    |
| <b>Réflexions sur le motif d'interception « protection économique »</b> . . . .                         | 59 |
| Les intérêts fondamentaux de la nation . . . . .                                                        | 60 |
| La sauvegarde des éléments essentiels du potentiel scientifique<br>et économique de la nation . . . . . | 61 |
| Les atteintes aux éléments essentiels du potentiel scientifique<br>et économique de la nation . . . . . | 61 |
| Chapitre V                                                                                              |    |
| <b>Interceptions de sécurité et secret défense</b> . . . . .                                            | 63 |

|                                       |    |
|---------------------------------------|----|
| Chapitre VI                           |    |
| <b>Jurisprudence</b> .....            | 65 |
| Jurisprudence européenne .....        | 65 |
| Jurisprudence française .....         | 70 |
| Chapitre VII                          |    |
| <b>Questions parlementaires</b> ..... | 75 |