

**COMITE PERMANENT DE CONTROLE DES
SERVICES DE RENSEIGNEMENT**

**RAPPORT D'ACTIVITES
1997**

Rue de la Loi, 52 – 1040 Bruxelles

02/286.28.11 – Fax : 02/286.29.99

A Monsieur le Président du Sénat,
A Monsieur le Président de la Chambre des Représentants,
A Monsieur le Ministre de la Justice,
A Monsieur le Ministre de la Défense Nationale,

Messieurs les Présidents,
Messieurs les Ministres,

En exécution de l'article 35 de la loi organique du 18 juillet 1991, instituant le contrôle des services de police et de renseignements, le Comité permanent de contrôle des services de renseignements à l'honneur de vous adresser en annexe le quatrième rapport général d'activités.

Ce rapport couvre la période du 1er octobre 1996 au 31 juillet 1997.

Nous vous prions de croire, Messieurs les Présidents, Messieurs les Ministres, en l'assurance de notre profonde considération.

Véronique Paulus de Châtelet
Présidente

Danielle Cailloux
Conseiller

Guy Collignon
Conseiller

Gérald Vande Walle
Conseiller

Wouter De Ridder
Greffier

ERRATUM

Le ministre de la Défense nationale nous a fait part des observations suivantes, auxquelles le Comité R adhère :

Page 147 : - Au SGR/CI :

il faut lire au lieu “des responsables de la section” - “les membres de la section”

Page 149 : - Au SGR/IH :

l'abréviation de la section exploitation doit être “IE” et non “EI”

Page 159 - point e

la phrase :

“Tout le personnel de cette section suit une formation à l'Ecole Royale Militaire”

doit être remplacée par :

“Tout le personnel suit une formation interne à ce sujet”.

RECAPITULATIF DES ACTIVITES DU COMITE

TITRE 1 : A L'ETRANGER

Etude de la législation néerlandaise sur les services de renseignement et de sécurité.....	- 12 -
Introduction.....	- 13 -

PREMIERE PARTIE

1. Service et organe définissant la politique à suivre.....	- 14 -
2. La base légale.....	- 14 -
3. Application de la loi.....	- 15 -
4. La coordination et la collaboration des services de renseignement et de sécurité.....	- 16 -
5. Les enquêtes de sécurité.....	- 17 -
6. La description des missions des services de renseignement et de sécurité.....	- 18 -
7. Compétence et méthode de travail des services.....	- 19 -
8. La communication de renseignements aux autorités compétentes.....	- 20 -
9. La collecte de données à caractère personnel par les services.....	- 21 -
10. L'obtention de données détenues par d'autres pouvoirs publics.....	- 23 -
11. restrictions au droit fondamental de quitter librement un pays.....	- 24 -
12. Collaboration avec les services de renseignement étrangers.....	- 25 -
13. Collaboration du ministère public et de la police avec les services.....	- 25 -
14. Confidentialité.....	- 26 -
15. Compétence des ministres concernés.....	- 27 -

16. Publication de rapports annuels.....	- 27 -
17. Le contrôle parlementaire sur les services de renseignement et de sécurité.....	- 28 -

DEUXIEME PARTIE

1. Le BVD.....	- 30 -
----------------	--------

TROISIEME PARTIE

1. Le MID	- 35 -
-----------------	--------

QUATRIEME PARTIE

Approche critique	- 39 -
1. La base légale.....	- 39 -
2. Faut-il une législation exhaustive sur les services de renseignement ? ...	- 40 -
3. Un service de renseignement spécifique compétent pour l'étranger ?.....	- 41 -
4. La coordination et la collaboration entre les services de renseignement, la collaboration entre le ministère public et la police, d'une part, et les services, d'autre part, la collaboration avec les services de renseignement étrangers.....	- 42 -
5. Les enquêtes de sécurité.....	- 43 -
6. La collecte de données à caractère personnel par les services.....	- 43 -
7. Droit de consultation d'un particulier.....	- 44 -
8. Restrictions au droit fondamental de quitter le territoire.....	- 45 -
9. Obligation de secret.....	- 45 -
10. La formation des fonctionnaires des services de renseignement et de sécurité.....	- 45 -
11. L'établissement d'un rapport annuel.....	- 45 -
12. Utilisation des sources ouvertes.....	- 45 -
13. Le contrôle parlementaire sur les services de renseignement et de sécurité.....	- 46 -

TITRE II : NOS SERVICES DE RENSEIGNEMENT

PREMIERE PARTIE : LES ÉTUDES - 47 -

Chapitre 1 : Audition des membres du Comité R devant les commissions réunies de la justice et de la défense nationale, le 7 janvier 1997

Introduction..... - 48 -

Chapitre 2 : Les droits d'accès du particulier à son dossier individuel auprès d'un service de renseignement

1. Introduction..... - 60 -
2. Motif de l'étude..... - 60 -
3. L'intérêt des parlementaires pour le problème..... - 60 -
4. Situation à l'étranger..... - 62 -
5. Les procédures d'accès dans la législation belge actuelle..... - 67 -
6. L'application de ces législations..... - 69 -
7. Projets et propositions de loi instaurant un droit de consulter des dossiers de la Sûreté de l'Etat..... - 74 -
8. Accès aux dossiers individuels via le Comité R..... - 75 -
9. Conclusions..... - 77 -
10. Recommandations..... - 78 -
11. Point de vue du ministre..... - 79 -

Chapitre 3 : Application de l'article 33 de la loi organique du 18 juillet 1991 par les services de renseignement

1. Introduction..... - 81 -
2. L'application de l'article 33, alinéa 2 par la Sûreté de l'Etat..... - 81 -
3. L'application de l'article 33, alinéa 2 par le SGR..... - 84 -
4. Conclusions..... - 86 -

DEUXIÈME PARTIE : LES ENQUÊTES

A. A la requête du Parlement ou des ministres

Chapitre 1 : Radioscopie du SGR..... - 88 -

Section 1 : Introduction..... - 88 -

1. Saisine du Comité R
2. Ouverture des enquêtes – procédure
3. Questions parlementaires déjà posées sur les sujets de l'enquête du Comité R

Section 2 : Les activités du SGR en général..... - 92 -

1. Aperçu historique
2. Activités actuelles du SGR

Section 3 : Les écoutes téléphoniques et les interceptions de communications auxquelles procéderaient le SGR..... - 97 -

1. Objet de l'enquête
2. Rétroactes de l'enquête
3. Les allégations de la presse
4. Questions et réponses parlementaires – déclarations officielles de ministres
5. L'enquête du Comité R
6. L'enquête judiciaire et la suspension de l'enquête du Comité R
7. Reprise de l'enquête par le Comité R
8. Les causes de justification en droit pénal
9. Conclusions
10. Recommandations

Section 4 : la réinstauration du réseau Stay-Behind..... - 107 -

1. Objet de l'enquête
2. Les allégations de la presse
3. Méthodologie
4. Historique du réseau Stay-Behind
5. Synthèse de l'enquête
6. Autres devoirs d'enquête
7. Conclusions

Section 5 : les cellules provinciales du SGR et leurs activités à l'égard des civils..... - 114 -

1. Introduction
2. Procédure
3. Fondement de l'enquête
4. Mise en place des cellules provinciales SGR/S (section CI)
5. Missions et méthodes de travail des cellules provinciales
6. Moyens des cellules provinciales
7. Lieux visités par le Comité R
8. Contrôle par le Service d'enquêtes au siège principal du SGR/CI
9. Conclusions

Chapitre 2 : Enquête sur la création éventuelle d'un nouveau service de renseignement militaire

- 121 -

1. Introduction
2. Procédure
3. Motif de l'enquête
4. Approche des différentes notions mentionnées dans le monde du renseignement
5. Synthèse de l'enquête
6. Evolution
7. Peut-on parler de la réinstauration du réseau Stay-Behind
8. Conclusions

B. A l'initiative du Comité

Chapitre 1 : Enquête de contrôle sur l'utilisation d'informateurs par la Sûreté de l'Etat et le SGR

- 139 -

1. Procédure
2. Fondement de l'enquête
3. L'intérêt porté au problème par le Parlement
4. Considérations préliminaires
5. Portée de l'enquête
6. Projets en cours d'exécution
7. Constatations
8. Recommandations
9. Conclusion générale

Chapitre 2 : Statuts des membres des services de renseignement..... - 168 -

Section 1 : Les statuts des membres du personnel du SGR..... - 168 -

Section 2 : Les agents contractuels de la Sûreté de l'Etat..... - 169 -

1. Poursuite de l'enquête – procédure
2. L'intérêt parlementaire pour le problème
3. Exposé de la situation
4. Les principes légaux applicables
5. Les arrêtés royaux d'application
6. Les fondements de l'engagement d'agents contractuels à la Sûreté de l'Etat
7. Les vérifications et constatations du service d'enquêtes
8. Conclusions
9. Recommandations
10. Echange de vue avec le ministre de la Justice

Chapitre 3 : la coordination des services de renseignement..... - 177 -

1. Procédure
2. Fondement de l'enquête
3. L'intérêt parlementaire pour le problème
4. Objet de l'enquête
5. Synthèse de l'enquête
6. Constatations
7. Recommandations

Chapitre 4 : Belinfosec..... -187 -

Ecoutes, prise de connaissance et enregistrement de communications et télécommunications privées et usage de la cryptographie en droit belge

1. Etat de la législation actuelle en matière de cryptographie
2. Proposition de solutions
3. Perspectives

C. Sur plaintes de particuliers ou sur dénonciation

Chapitre 1 : Enquête de contrôle suite à la plainte déposée par monsieur X..... - 204 -

1. Procédure
2. Déroulement de l'enquête
3. Conclusions

Chapitre 2 : Enquête de contrôle suite à la plainte déposée par monsieur Y..... - 206 -

1. Procédure
2. Synthèse de l'enquête
3. Constatations
4. Conclusions
5. Recommandation

D. Enquête commune des Comités P et R

Enquête commune relative à la destruction éventuelle de documents provenant de la police judiciaire par le service général de renseignement et de sécurité (SGR)..... - 210 -

1. Introduction
2. Procédure
3. Origine de l'enquête
4. Synthèse de l'enquête
5. Constatations
6. Recommandations à l'égard de la police judiciaire

TITRE III : CONTACTS DU COMITE

Chapitre 1 : Congrès de Washington..... - 226 -

A. Infowarcon

B. Open sources solutions

C. Law Enforcement and Intelligence

1. Introduction
2. Objet du Congrès
3. Différences habituelles entre « Intelligence » et « Law Enforcement »
4. Situation pendant et après la Guerre Froide
5. Situation actuelle
6. Mesures pour anticiper l'évolution de la nouvelle situation
7. Législation – problématique
8. Collaboration internationale
9. Conclusions

Chapitre 2 : Europe horizon 2000 : nouvelles menaces, nouveaux terrorismes..... - 238 -

Chapitre 3 : Séminaire « Internet face au droit »..... - 241 -

Chapitre 4 : Rencontre du Comité R avec la délégation ukrainienne..... - 243 -

Chapitre 5 : Colloque sur l'intelligence économique à Paris..... - 245 -

Chapitre 6 : Contacts du Comité R avec le BVD et le MID..... - 250 -

Chapitre 7 : colloque « Terrorisme et prolifération »..... - 251 -

Chapitre 8 : Congrès Infowarcon à Bruxelles.....- 253 -

TITRE IV : EVOLUTION DU COMITE

1. La composition du Comité R..... - 257 -
2. Les activités du Comité..... - 257 -
3. Les moyens financiers..... - 258 -
4. Activités communes avec le Comité P..... - 259 -

Titre V : RECOMMANDATIONS

Bilan 1997 de quatre années de contrôle et de recommandations..... - 261 -
1. Une loi organique sur les services de renseignement.....- 261 -
2. La protection des droits des citoyens..... - 262 -
3. L'efficacité des services de renseignement..... - 264-

TITRE I : A L'ETRANGER

ETUDE DE LA LEGISLATION NEERLANDAISE SUR LES SERVICES DE RENSEIGNEMENT ET DE SECURITE

INTRODUCTION

Dans son rapport d'activités de 1995, le Comité R publiait une étude relative à "la comparaison de certaines législations étrangères" en matière de services de renseignement.

Dans le rapport annuel de 1996, il analysait en profondeur la législation allemande sur les services de renseignement et les organes de contrôle.

Dans le présent rapport, le Comité R approfondit la législation néerlandaise en matière de services de renseignement et de contrôle de ses services.

Le système néerlandais est proche du système belge, car les Pays-Bas comptent également deux services de renseignement, un civil : **BVD** (Binnenlandse Veiligheidsdienst) qui est l'équivalent de la Sûreté de l'Etat belge et un service de renseignement militaire : **MID** (Militaire inlichtingendienst) qui est l'équivalent du SGR belge.

Un contrôle parlementaire est exercé par la : "Commissie voor de Inlichtingen- en Veiligheidsdiensten van de Tweede Kamer" . Le rapport de la Commission est discuté chaque année en séance plénière par la "Tweede Kamer".

Dans la première partie de cette étude, nous aborderons la législation s'appliquant aux différents services de renseignement et de sécurité.

Dans la deuxième partie, sont approfondies les caractéristiques plus spécifiques du BVD et, dans la troisième partie, celles du MID.

Le Comité R a demandé par écrit au ministre néerlandais de l'Intérieur l'autorisation d'effectuer un voyage d'étude auprès du BVD.

Le ministre a donné son accord, en précisant que les sujets opérationnels ne pouvaient faire l'objet d'aucune discussion.

Durant ce voyage d'étude, le Comité R a été informé de la réglementation en vigueur. Ce dernier a également pu assister à une démonstration de l'utilisation des sources ouvertes. Les matières opérationnelles n'ont pas été abordées, conformément au souhait du ministre de l'Intérieur.

L'autorisation de rendre visite au MID a été demandée au ministre néerlandais de la Défense. Cette autorisation nous a été accordée aux mêmes conditions que pour le BVD.

PREMIERE PARTIE

1. SERVICES ET ORGANE DEFINISSANT LA POLITIQUE A SUIVRE

1.1. Nombre de services de renseignement et de Sécurité

Les Pays-Bas comptent deux services de renseignement et de sécurité, à savoir le BVD et le MID, placés respectivement sous la responsabilité du ministère de l'Intérieur et du ministère de la Défense.

Jusqu'au 1^{er} janvier 1994, les Pays-Bas disposaient encore du “IDB” (Inlichtingendienst Buitenland), supprimé par la loi du 2 décembre 1993 (*cf. point 2.2*).

1.2. La Commission ministérielle pour les services de renseignement et de sécurité

Depuis 1976, il existe au niveau gouvernemental une “Commission ministérielle pour les services de renseignement et de sécurité” (MICIV). Cette commission a été instituée par arrêté ministériel et a pour mission de définir la politique générale des services de renseignement et de sécurité ainsi que la coordination de ces services.

Le Premier ministre préside cette Commission, composée du ministre des Affaires étrangères, du ministre de la Justice, du ministre de l'Intérieur, du ministre des Finances, du ministre de la Défense et du ministre des Affaires économiques.

2. LA BASE LEGALE

2.1. La loi du 3 décembre 1987 sur les services de renseignement et de sécurité

Ces services fonctionnent sur une base légale, à savoir la loi du 3 décembre 1987, portant sur les règles relatives aux services de renseignement et de sécurité (loi sur les services de renseignement et de sécurité - WIV).

Lors de l'adoption de cette loi, on est parti du principe qu'une réglementation légale devait non seulement porter sur le BVD, mais également sur tous les services de renseignement et de sécurité cités dans la loi.

La loi prévoit, par conséquent, des dispositions qui sont aussi bien applicables au BVD qu'au MID (et, à l'origine, également au IDB). Cette loi est entrée en vigueur le 1^{er} février 1988.

2.2. Modification de la loi le 2 décembre 1993

Cette loi a été modifiée par la loi du 2 décembre 1993, entrée en vigueur le 1^{er} janvier 1994. Elle met fin à l'existence de l'IDB.

A la suite de la suppression de l'IDB, certaines de ses activités ont été abandonnées. Certaines de celles-ci ont été reprises par le MID et le BVD car elles sont décrites dans leurs missions légales.

Ces activités concernent notamment :

- le maintien de contacts avec les services étrangers concernés;
- l'exercice de missions de défense ad hoc par le MID;
- l'exécution de missions opérationnelles nécessaires avec une orientation internationale par le BVD, pour autant qu'elles soient liées à la sécurité ou à d'autres intérêts importants de l'Etat;
- le traitement des données obtenues.

2.3. Nouvelle modification de la loi

Le 16 juin 1994, la section administrative du Conseil d'Etat, dénommée ci-après la "Section", a rendu un arrêt dans les affaires Van Baggum et Valkenier, qui opposait les demandeurs au ministre de l'Intérieur.

La "Section" a estimé que l'article 16 de la loi sur les services de renseignement et de sécurité, qui régit (entre autres) la publicité des données à caractère personnel dans les dossiers de renseignement et de sécurité, était inapplicable, car il est contraire aux articles 8 et 13 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales.

La "Section" a annulé, dans les deux affaires, la décision du ministre de l'Intérieur. Ces arrêts ont provoqué l'élaboration d'un projet de modification de la loi sur les services de renseignement et de sécurité. Le projet de loi est toujours en cours de discussion.

3. APPLICATION DE LA LOI

L'article 2 de la loi sur les services de renseignement et de sécurité stipule que :

"De coördinator en de diensten verrichten hun taak in gebondenheid aan de wet en in ondergeschiktheid aan onze betrokken minister".

3.1. L'application des dispositions légales

La lecture de l'exposé des motifs permet de mieux comprendre la volonté du législateur . La règle fondamentale veut que les services soient soumis, dans l'exécution de leurs missions, aux dispositions légales qui s'appliquent à tout acte posé par les pouvoirs publics.

Ce n'est que lorsqu'il est absolument nécessaire pour l'exécution de leur mission, et alors uniquement conformément à ou en vertu de la loi, que des compétences particulières peuvent être attribuées aux services, comme par exemple, les compétences prévues par l'article 139a du Code pénal.

L'article 139 points a), b) et c) du Code pénal punit la mise sur écoute téléphonique ainsi que l'enregistrement et la mise sur écoute au moyen d'un appareillage technique de conversations dans des habitations, des locaux fermés ou ailleurs. Cependant, cet article prévoit des exceptions pour le BVD (*cf. point 7.2*).

3.2. La tutelle du ministre compétent

Les services exercent leurs activités sous l'autorité du ministre compétent.

Les services dépendent, pour toutes les facettes de l'exercice de leur mission, du ministre concerné, lui-même pleinement responsable sur le plan politique devant le Parlement.

Les ministres concernés sont chacun individuellement responsables de la politique qu'ils mènent à l'égard des services qui leur sont subordonnés.

4. LA COORDINATION ET LA COLLABORATION DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ

Cette matière est régie par les articles 3 à 7 de la loi sur les services de renseignement et de sécurité.

4.1. Le coordinateur

La loi prévoit la fonction de coordinateur des services de renseignement et de sécurité. Celui-ci est désigné sur proposition collective du Premier ministre, du ministre des Affaires générales, et des ministres de l'Intérieur et de la Défense et est nommé par arrêté royal (article 5 de la loi).

Ce coordinateur a pour mission de, conformément aux indications du Premier ministre, et en accord avec les ministres de l'Intérieur et de la Défense :

- préparer la commission ministérielle sur les services de renseignement;
- coordonner l'exécution des missions des services ;
- présenter aux ministres certaines propositions concernant l'exécution des missions des services.

La préparation de la concertation ministérielle porte essentiellement sur les grandes lignes de la politique générale de renseignement.

4.2. Le CVIN (Comité Verenigde Inlichtingendiensten Nederland)

Le CVIN a été constitué par arrêté ministériel et se réunit en principe chaque mois.

Il discute, avec les responsables du BVD et du MID, ainsi qu'avec les hauts fonctionnaires des ministères de la Justice et des Affaires étrangères, de la politique des services de renseignement.

Le coordinateur est également président du Comité Verenigde Inlichtingendiensten Nederland et, de ce fait, il favorise la collaboration entre les différents services et le gouvernement.

4.3. CVIN - Plus

Le CVIN-Plus se réunit pour préparer la commission ministérielle (de Ministeriële Commissie voor de Inlichtingen- en Veiligheidsdiensten - MICIV).

Il fait office d'antichambre administrative du MICIV.

Il regroupe les membres du CVIN des Pays-Bas et les secrétaires généraux des ministres qui sont membres du MICIV.

4.4. Devoirs des responsables des Services à l'égard du coordinateur

Le coordinateur doit disposer de tous les renseignements souhaités pour une bonne exécution de ces missions et pour prendre l'initiative de fournir aux ministres concernés les informations utiles dans le cadre de la politique générale de renseignement.

L'article 6 de la loi prévoit, en effet :

" *De hoofden van de diensten verlenen de coördinator medewerking voor de uitoefening van zijn taak. Zij zijn gehouden hem daartoe alle nodige gegevens te verschaffen*".

4.5. Collaboration entre les services

L'article 13 de la loi prévoit que les services doivent, autant que possible, collaborer ensemble notamment par l'échange d'informations.

Cette disposition se situe dans le prolongement des travaux du coordinateur. Une intervention efficace des services exige qu'ils collaborent autant que possible entre eux, notamment en échangeant les informations qu'ils recueillent.

5. LES ENQUETES DE SECURITE

5.1. Mentions dans la loi sur les services de renseignement et de sécurité (WIV)

Dans la loi sur les services de renseignement et de sécurité, il est prévu que le BVD et le MID mènent des enquêtes de sécurité sur l'exercice de fonctions de confiance ou de fonctions dans le monde économique qui pourraient, de l'avis des ministres compétents, nuire à la sécurité ou à d'autres intérêts vitaux de l'Etat (article 8, 2b pour le BVD et l'article 9, 2b pour le MID).

La désignation des fonctions de confiance se fait surtout sur base de deux principes.

Il s'agit de :

- la possibilité de pouvoir prendre connaissance d'informations liées à des secrets d'Etat ;

- la réalisation de travaux relatifs à des secteurs des pouvoirs publics et du monde économique qui présentent un intérêt vital pour la défense du pays ou le maintien de la vie en société.

Le BVD a également pour mission de favoriser la protection de ces informations et les secteurs spécifiques des pouvoirs publics et du monde économique qui sont, de l'avis des ministres compétents, d'un intérêt vital pour le maintien de la vie en société.

Le MID remplit la même mission, mais orientée vers les forces armées.

5.2. Loi sur les enquêtes de sécurité (WVO)

Jusqu'il y a peu, il n'existait aucun règlement uniforme pour l'ouverture d'une enquête de sécurité sur des personnes qui occupent une fonction de confiance dans le secteur public ou privé.

Le « Staatsblad van het Koninkrijk Nederland » 1996 nr. 525 a publié la loi du 10 octobre 1996 sur les enquêtes de sécurité (WVO).

Les services de renseignement continuent à mener les enquêtes de sécurité, mais dans la loi sur les enquêtes de sécurité, l'article 2 prévoit clairement dans quels cas ces enquêtes peuvent être menées par le MID. D'autre part, la loi définit les modalités d'exécution de ces enquêtes.

Il existe des moyens juridiques ⁽¹⁾ pour s'opposer au refus de délivrer une "attestation de non-objection" (art.8, WVO) ainsi qu'au "retrait d'une attestation" (art.10, WVO). Ces décisions sont considérées comme des arrêtés au sens de l'article 1 :3, premier alinéa de la loi générale sur le droit administratif (AWB).

Cette loi prévoit une procédure de réclamation auprès de l'organe administratif qui a pris la décision ainsi qu'une possibilité d'interjeter appel auprès du juge administratif, avec une possibilité d'appel en second degré.

La loi est entrée en vigueur le 1^{er} février 1997.

6. LA DESCRIPTION DES MISSIONS DES SERVICES DE RENSEIGNEMENT ET DE SECURITE

Cette description se retrouve à l'article 8 (pour le BVD) et à l'article 9 (pour le MID) de la loi sur les services de renseignement et de sécurité.

6.1. Article 8 - en ce qui concerne le BVD

- La collecte de données sur des organisations et des personnes qui, par les buts qu'elles se fixent ou par leurs activités, permettent de supposer sérieusement qu'elles représentent un

(1) "Attestation de non-objection" signifie accepter l'octroi d'un certificat de sécurité et le "retrait d'une attestation" est la perte d'un certificat de sécurité.

danger pour la démocratie, la sécurité ou pour d'autres intérêts vitaux de l'Etat ;

- L'exécution d'enquêtes de sécurité (cf. point 5);
- Favoriser des mesures de protection des données dont la confidentialité s'impose dans l'intérêt de l'Etat, des secteurs des pouvoirs publics et du monde économique et qui sont, de l'avis des ministres compétents, d'un intérêt vital pour le maintien de la vie en société.

6.2. Article 9 - en ce qui concerne le MID

- La collecte de données sur le potentiel et les forces armées d'autres puissances, qui sont nécessaires pour assurer l'adéquation de la structure des forces armées et l'efficacité de son utilisation ;
- L'exécution d'enquêtes de sécurité (cf. point 5);
- La collecte de données nécessaires pour prendre des mesures :
 - a. de prévention des activités qui visent à nuire à la sécurité ou à la capacité d'intervention des forces armées ;
 - b. de protection des données relatives aux forces armées dont la confidentialité s'impose;
 - c. pour favoriser le bon déroulement de la mobilisation et de la concentration des forces armées.

7. COMPETENCES ET METHODE DE TRAVAIL DES SERVICES

7.1. Généralités

L'article 1, alinéa 2 de la loi, définit un "fonctionnaire" comme une personne qui exécute un "*contrat de travail en droit civil.*" ⁽²⁾

L'article 20 de la loi sur les services de renseignement et de sécurité dispose que les fonctionnaires des services ne possèdent aucune compétence pour rechercher des faits délictueux.

Cette exception a été reprise dans la loi, car elle constitue une garantie particulière afin que les services se limitent au domaine qui leur est dévolu par la loi.

Cet article implique donc que ces fonctionnaires ne possèdent pas la qualité d'officier de police judiciaire.

Le travail de ces services consiste à recueillir, enregistrer et analyser des informations, provenant soit de sources ouvertes, soit de sources fermées. Ils collaborent, aussi bien entre eux qu'avec des

⁽¹⁾ Traduction libre

services alliés étrangers, dans le but d'informer les autorités compétentes, en temps utile, des menaces éventuelles qui pèsent sur la sécurité ou d'autres intérêts vitaux de l'Etat, et en ce qui concerne le MID, au sujet du potentiel des forces armées d'autres puissances et de la sécurité des forces armées.

Les services disposent de directives internes confidentielles relatives à l'exécution de leurs tâches opérationnelles.

7.2. Méthodes particulières des services

Sur base de l'article 15, les services peuvent s'adresser à n'importe qui pour obtenir des informations.

Seul le BVD peut écouter des conversations téléphoniques, les enregistrer et écouter, à l'aide d'appareils, des conversations dans des habitations, des locaux fermés ou d'autres lieux.

Le BVD peut également capter des données transférées par ordinateur.

Cette opération n'est autorisée qu'avec l'accord de quatre ministres, à savoir le Premier ministre, le ministre de l'Intérieur, le ministre de la Justice et le ministre des Communications et des Ponts et Chaussées. Toutefois, dans le cas de la mise sur écoute de conversations dans des habitations, seul l'accord de trois d'entre eux est requis, à savoir : le Premier ministre et les ministres de l'Intérieur et de la Justice.

Cette matière est régie par le Code pénal.

D'autres méthodes sont utilisées pour collecter des données, comme la filature et l'observation de personnes. Le recours à ces techniques est légitimé par la mission légale. Cependant, un fondement légal spécifique n'est pas (encore) repris dans la loi.

Le cabinet a déclaré qu'il définirait clairement, lors de la modification de la loi sur les services de renseignement et de sécurité, les méthodes, comme la filature et l'observation, avec ou sans appareillage d'observation et de localisation.

8. LA COMMUNICATION DE RENSEIGNEMENTS AUX AUTORITES COMPETENTES

8.1. Au ministre compétent

Le responsable d'un service est légalement tenu d'informer en permanence le ministre compétent de tout élément qui peut présenter un intérêt (article 11, 1^{er} alinéa).

Le ministre responsable doit se justifier, à son tour, devant le parlement à propos des activités d'un service.

La Commission des services de renseignement et de sécurité est, quant à elle, informée des opérations.

Le responsable du service apporte, à cet égard, une assistance administrative au ministre.

8.2. A d'autres autorités

Par ailleurs, tous les services peuvent, dans l'exercice de leur mission, recueillir des informations pouvant présenter un intérêt non seulement pour le ministre responsable concerné, mais également pour d'autres ministres.

L'article 11, 2^{ème} alinéa établit comme règle fondamentale que le ministre concerné transmet sans délai les données au ministre intéressé.

8.3. Mandat de longue durée accordé au responsable du Service

Diffuser le renseignement à d'autres organes du pouvoir ou à d'autres ministres, en le communiquant d'abord au ministre concerné peut retarder la transmission d'informations urgentes et importantes.

Dans cette optique, l'article 12 prévoit la possibilité d'accorder un mandat de longue durée au responsable d'un service afin qu'il puisse communiquer des informations à d'autres ministres aux organes du pouvoir et aux services publics.

9. LA COLLECTE DE DONNEES A CARACTERE PERSONNEL PAR LES SERVICES

9.1. Règlement pour les données à caractère personnel conservées par les Services

La loi "wet Persoonsregistraties", relative à la documentation établie à propos de particuliers par les pouvoirs publics et par les entreprises privées, ne s'applique pas aux données à caractère personnel conservées par ou au bénéfice des services de renseignement et de sécurité (article 2 de la loi "wet Persoonsregistraties").

La nature et le caractère particulier de cette documentation établie par les services de renseignement expliquent cette exception. Ces dossiers tombent sous l'application de la loi sur les services de renseignement et de sécurité (articles 16 et 17).

L'article 16, 1^{er} alinéa, érige en principe que les services peuvent recueillir, tenir une documentation et communiquer à des tiers uniquement des données à caractère personnel nécessaires pour l'exécution des missions décrites dans cette loi.

9.2. Règles à fixer par le ministre compétent et le ministre de la Justice

L'article 16, 3ème alinéa stipule que le ministre compétent, en accord avec le ministre de la Justice, particulièrement compétent en matière de protection de la vie privée, fixe les règles concernant la gestion de données à caractère personnel conservées par le service.

9.3. Prescriptions obligatoires

L'article 16, 4ème alinéa stipule que les règles visées à l'alinéa précédent doivent au moins traiter :

- 1) des objectifs poursuivis lors de la collecte de données à caractère personnel ⁽¹⁾ ;
- 2) de la confidentialité des données enregistrées ;
- 3) du contrôle de l'exactitude de ces données ;
- 4) des délais pendant lesquels les données enregistrées peuvent être conservées ;
- 5) des autres motifs de sélection de données recueillies ;
- 6) de la destruction de données sélectionnées.

Les règles visées aux points 2) et 3) sont fixées respectivement dans le "Privacy-regeling Binnenlandse Veiligheidsdienst" et le "Privacy-regeling Militaire inlichtingendienst" (Staatscourant 1988, p. 126).

9.4. Droit de consultation par un particulier

L'article 16, 2ème alinéa, de la loi sur les services de renseignement et de sécurité stipule qu'en règle générale, les particuliers n'ont pas accès aux enregistrements effectués par un service.

Cela implique que les gestionnaires ont l'obligation de veiller eux-mêmes à l'exactitude des données à caractère personnel répertoriées.

Enfin, il faut noter le fait que la section administrative du Conseil d'Etat a décidé, dans les affaires Van Baggum et Valkenier, que l'article 16 de la loi sur les services de renseignement et de sécurité, qui régit, entre autres, la publicité des dossiers du BVD et du MID, ne devait pas être appliqué, parce que contraire aux articles 8 et 13 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (*cf. point 2.3⁽¹⁾*).

9.5. Consultation de données à caractère personnel par les services

L'article 17, 1^{er} alinéa, prévoit que les services sont habilités à s'adresser au gestionnaire d'une banque de données à caractère personnel pour obtenir la communication desdites données dans

⁽¹⁾ Il s'agit d'une disposition essentielle, car elle contraint les personnes qui détiennent un ensemble de données personnelles à déterminer, au regard des tâches du service concerné, si l'enregistrement de certaines données est nécessaire et/ou autorisé.

⁽²⁾ Voir titre II - première partie - chapitre 2 ("Accès aux dossiers des services de renseignement par un particulier")

les cas suivants :

- a. pour les besoins d'une enquête de sécurité relative à l'exercice d'une fonction de confiance;
- b. dans les cas ou type de cas définis dans un mandat délivré conjointement par le ministre compétent et celui de la Justice.

Si les services souhaitent l'accès à des enregistrements de données à caractère personnel, dans le cadre de certains travaux (cas visés au point b.), ils doivent disposer d'une autorisation du ministre concerné et du ministre de la Justice.

Ce mandat ⁽¹⁾ peut être valable pour des cas déterminés ou pour certains types de cas. A l'article 17, 2ème alinéa, il est indiqué que l'autorisation mentionne la période de validité. Cette période ne peut dépasser un an, à compter de la date de délivrance de l'autorisation.

9.6. La communication de données à caractère personnel aux services

L'article 17, 3ème alinéa, prévoit que les prescriptions légales en vigueur pour le titulaire d'une banque de données à caractère personnel, relatives à la communication de ces données, ne sont pas applicables aux communications faites à la suite d'une demande visée au 1^{er} alinéa.

Cela signifie, entre autres, que les dispositions légales de la loi "wet Persoonsregistraties" sur la communication de données à caractère personnel ne sont pas applicables dans l'hypothèse où une autorité publique ou une entreprise a fourni, des données à caractère personnel au BVD ou au MID, à leur demande.

9.7. Exception pour les données judiciaires

L'article 17, 4ème alinéa, prévoit une exception pour les données recueillies en vertu de la loi sur "De Justitiële documentatie en de verklaringen omtrent het gedrag verzameld justitiële gegevens".

L'arrêté "Justitiële Documentatie" du 23 septembre 1958, basé sur l'article 13 de cette loi, prévoit déjà une disposition particulière pour l'accès des services à ces données.

10. L'OBTENTION DE DONNEES DETENUES PAR D'AUTRES POUVOIRS PUBLICS

10.1. Compétence des Services

Le coordinateur et les responsables des services sont compétents pour s'adresser à d'autres pouvoirs publics afin d'obtenir les données nécessaires à l'exercice leurs activités (article 15).

Ici, il convient de souligner que la compétence attribuée par cet article ne déroge pas à l'application

⁽¹⁾ Un mandat peut être assimilé à une autorisation.

d'autres dispositions légales en vigueur sur l'accès aux données à caractère personnel, comme par exemple celles concernant le secret des correspondances.

10.2. Concertation entre le BVD et le MID

L'exposé des motifs de la loi mentionne que le MID devra avoir accès aux données indispensables pour l'exécution de sa mission de sécurité.

Afin d'éviter que les autorités publiques exécutent le même travail à deux reprises, il est indispensable que le MID se concertent avec le responsable du BVD (cf. voir point 4.5. - art. 13).

11. RESTRICTIONS AU DROIT FONDAMENTAL DE QUITTER LIBREMENT UN PAYS

11.1. Le droit fondamental de quitter librement le pays

Le droit fondamental de quitter librement un pays est garanti par le droit public international. L'exercice de ce droit ne peut être soumis à aucune restriction, si ce n'est celles prévues par la loi et rendues nécessaires, pour des motifs énoncés de manière limitative.

Ainsi, l'article 2, 2ème alinéa, du quatrième protocole de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales mentionne, entre autres, comme motifs de restriction: la sécurité du pays, la sécurité publique et la prévention d'actes délictueux (Exposé des motifs - "Tweede Kamer", la loi sur les services de renseignement et de sécurité).

11.2. Restrictions imposées par la loi sur les services de renseignement et de sécurité

C'est ainsi que l'on trouve dans la loi sur les services de renseignement et de sécurité une base légale restreignant la liberté de voyager.

L'article 21 impose certaines restrictions aux fonctionnaires, comme partir ou séjourner dans un pays en conflit armé.

Ainsi, un arrêté royal peut indiquer les pays où le séjour des fonctionnaires des services présenterait des risques inacceptables pour la sécurité ou les intérêts vitaux de l'Etat.

Cette restriction à la liberté de quitter le pays s'applique également aux fonctionnaires de police qui effectuent des travaux pour le BVD (en ce qui concerne ces fonctionnaires, voir point 13.1) ainsi qu'au coordinateur et aux fonctionnaires qui lui sont subordonnés.

Il ressort de l'exposé des motifs de la loi que cette restriction est inspirée par le fait qu'il est apparu à plusieurs reprises que des services de renseignement de pays non démocratiques accordent une grande priorité à l'infiltration des services de renseignement et de sécurité des démocraties occidentales.

De ce fait, les collaborateurs des services de renseignement et de sécurité courent un risque considérable lors de séjours dans un de ces pays. D'une part, on ne peut exclure le fait que les agents des services de renseignement soient connus comme tels.

D'autre part, en raison précisément de ces fonctions, ces agents ont accès à des données sensibles pour la sécurité de leurs pays et de celles de leurs alliés. Enfin, ceci pourrait mettre en danger la sécurité des collaborateurs des services de renseignement.

11.3. Levée de cette interdiction

Le ministre compétent peut lever cette interdiction si des intérêts personnels impérieux du fonctionnaire le commandent et si la sécurité ou d'autres intérêts vitaux de l'Etat ne s'y opposent pas.

12. COLLABORATION AVEC LES SERVICES DE RENSEIGNEMENT ETRANGERS

Pour assurer l'efficacité de l'intervention des services, il peut s'avérer nécessaire de collaborer avec des services d'autres puissances.

L'article 13, 2ème alinéa, en accorde l'autorisation :

"De hoofden van de diensten dragen zorg voor het onderhouden van verbindingen met daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere mogend-heden".

13. COLLABORATION DU MINISTERE PUBLIC ET DE LA POLICE AVEC LES SERVICES

Cette matière est régie par l'article 22 de la loi sur les services de renseignement et de sécurité.

13.1. Communication de données par le Ministère public et les services de police

Les membres du ministère public et des services de police prennent régulièrement connaissance, dans l'exercice de leur fonction, de faits et d'informations de nature à intéresser la bonne exécution des missions confiées aux services de renseignement et de sécurité. Toutefois, il n'est pas souhaitable que ces fonctionnaires les communiquent directement et librement aux services de renseignement et de sécurité.

C'est pourquoi, l'article 22, 1^{er} alinéa, de la loi sur les services de renseignement et de sécurité prévoit que les membres du Ministère public effectuent la communication susvisée par l'intermédiaire du Procureur général. Quant aux services de police l'alinéa 2 prévoit qu'ils communiquent ces données à leur chef de corps. Ce dernier transmet les données au service s'il estime qu'elles présentent un intérêt.

13.2. Concertation entre le Ministère public et les services de renseignement

L'article 22, 3ème alinéa de la loi sur les services de renseignement et de sécurité prévoit une concertation régulière entre le Ministère public et un service :

" *Steeds wanneer de vervulling van de taak van het Openbaar Ministerie en van een dienst daartoe aanleiding geeft, plegen de betrokken Procureur-generaal en het hoofd van de betrokken dienst overleg.*"

La lecture de l'exposé des motifs de la loi apprend que l'expérience acquise à l'occasion de la lutte contre le terrorisme a démontré l'importance de la rapidité de la diffusion d'une information au stade de la préparation d'une infraction aux autorités chargées de la recherche et de la poursuite de faits délictueux. Il en est de même en ce qui concerne la lutte contre l'espionnage et le sabotage. Dans l'intérêt de la prévention, il est essentiel que le ministère public soit immédiatement averti de la préparation de telles infractions graves. L'intérêt d'une telle concertation (prévue par l'article 22 - 3ème alinéa) est donc évidente.

14. CONFIDENTIALITE

Cette matière est régie par les articles 14, 23 et 24 de la loi sur les services de renseignement et de sécurité.

14.1. Article 14 de la loi

"Le coordinateur et les responsables des services veillent à :

- a) *de geheimhouding van daarvoor in aanmerking komende gegevens en van de bronnen waaruit die afkomstig zijn;*
- b) *de veiligheid van personen met wier medewerking die gegevens worden verzameld*".

Le devoir de confidentialité mentionné au point a) ne s'applique pas à l'égard du ministre concerné et ce en raison de sa responsabilité politique. Pour pouvoir s'exercer pleinement, cette dernière exige que le ministre compétent ait accès sans restriction à toutes les informations détenues par le service de renseignement.

Les obligations évoquées ici tendent à garantir non seulement la sécurité des informateurs, mais vise aussi la protection des fonctionnaires des services. Les relations des agents des services avec les informateurs sont confidentielles.

14.2. Article 23 de la loi

Cet article stipule que toute personne concernée par l'exécution de cette loi et qui dispose ainsi de données dont il connaît le caractère confidentiel ou devrait raisonnablement le supposer, est tenue au secret, sauf dans la mesure où une prescription légale le contraint à le dévoiler.

Cette obligation subsiste même après que la personne ne soit plus concernée par l'application de cette loi. Ce devoir de secret incombe également aux fonctionnaires qui, bien qu'ils ne soient pas directement concernés par les activités du service, détiennent des données dont la confidentialité est d'un intérêt essentiel pour la sécurité de l'Etat.

Cela peut être le cas en cas d'application des articles 11 et 12 de cette loi, c'est-à-dire lorsque les services transmettent des données à d'autres ministères ou aux autorités publiques.

14.3. Article 24 - exceptions à l'obligation de secret

L'obligation de secret ne s'applique pas à l'égard de la personne dont le fonctionnaire est le subordonné, ni dans le cas où le fonctionnaire a été déchargé de cette obligation par un supérieur.

Un fonctionnaire contraint, en vertu d'une prescription légale, de comparaître à l'occasion d'une procédure judiciaire comme témoin ou expert, ne peut faire de déclaration sur des éléments couverts par son devoir de secret, conformément à l'article 24, sauf si le ministre compétent et le ministre de la Justice l'ont conjointement déchargé par écrit de cette obligation.

Un conflit peut survenir entre les intérêts de la sécurité nationale, qui peut exiger la confidentialité de certaines sources ou données, et l'intérêt de la recherche de la vérité dans une procédure civile ou pénale.

Dans les cas où des fonctionnaires d'un service sont convoqués comme témoins, les intérêts en présence seront mis en balance, cas par cas.

A cet égard, il faudra examiner si l'intérêt de la sécurité nationale in concreto tolère ou ne tolère pas, que l'intéressé soit levé de son devoir de secret. Pour veiller à ce que la balance des intérêts en jeu respecte la pondération nécessaire, il est prévu que la levée du devoir de secret relève conjointement du ministre concerné et du ministre de la Justice.

15. COMPETENCE DES MINISTRES CONCERNES

L'article 19 de la loi dispose :

" *Omtrent de organisatie, de werkwijze en het beheer van een dienst kunnen nadere regels worden gesteld door onze betrokken Minister*".

Le législateur a voulu ainsi exprimer que seul le ministre responsable d'un service est compétent pour fixer des règles plus précises pour l'organisation, la gestion et la méthode de travail de ce service.

16. PUBLICATION DE RAPPORTS ANNUELS

Le BVD publie un rapport annuel public. Dans ces rapports annuels, il est fait mention des phénomènes concrets qui exigent l'attention des services. Les données secrètes, opérationnelles ne sont pas reprises dans la partie publique du rapport annuel.

Le MID ne publie pas (encore) de rapport annuel.

17. LE CONTROLE PARLEMENTAIRE SUR LES SERVICES DE RENSEIGNEMENT ET DE SECURITE

17.1. La responsabilité ministérielle

Les ministres compétents pour les services de renseignement et de sécurité doivent en répondre devant le parlement.

Cette responsabilité s'étend à toutes les activités du service ainsi qu'à la gestion de son budget. Par conséquent, le parlement est compétent pour contrôler les activités des services de renseignement et de sécurité par l'intermédiaire des ministres responsables.

En général, comme c'est d'ailleurs aussi le cas pour les autres ministères, le parlement peut demander au ministre compétent de fournir des informations sur le service de renseignement et ses activités. Le ministre est tenu de fournir les informations demandées, à moins que l'intérêt de l'Etat ne permette pas de les rendre publiques.

Dans le cas où le ministre est convaincu que la divulgation d'une information peut présenter un danger pour l'intérêt de l'Etat, il peut refuser de divulguer cette information au parlement (on peut penser ici à des informations sur des sources ou sur un modus operandi particulier). Il n'empêche que le ministre est tenu d'expliquer au parlement pourquoi il estime que la divulgation de certaines informations compromettrait l'intérêt de l'Etat.

17.2. Constitution en 1952 d'une "Vaste Commissie voor de Inlichtingen- en Veiligheidsdiensten in de Tweede Kamer"

Pour éviter que le gouvernement néerlandais ne doive faire appel à la procédure précitée, le parlement a cherché des alternatives.

En 1952, une "Vaste Commissie voor de Inlichtingen- en Veiligheidsdiensten" a été constituée pour la première fois à la "Tweede Kamer". Elle réunit les présidents des quatre principaux groupes politiques de la "Tweede Kamer".

17.3. Dénomination et composition actuelles

Cette Commission se compose actuellement, comme nous l'avons indiqué plus haut, des présidents de groupe des quatre principaux partis politiques (opposition comprise). Elle porte actuellement le nom de "Commissie voor de Inlichtingen- en Veiligheidsdiensten van de Tweede Kamer".

Cette Commission organise elle-même son travail et adopte son propre règlement d'ordre intérieur. La présidence est assurée par le président du principal groupe représenté au parlement. La Commission travaille à huis clos. Ses membres sont tenus au secret. Cette obligation subsiste même après la fin de leur mandat.

17.4. Missions et méthode de travail

Le nombre de réunions qui doivent être tenues par la Commission n'est pas prévu. Une concertation régulière des présidents de groupe avec les ministres responsables des services a conduit à une pratique où presque tous les aspects de la mission des services, leur organisation et leur méthode de travail font ou peuvent faire l'objet de discussions.

La Commission peut également exercer un contrôle sur le budget des services. Mais c'est surtout une mission qui revient à la "Algemene Rekenkamer". En vertu de la loi sur la comptabilité, le président de la "Algemene Rekenkamer" contrôle personnellement le budget secret des services.

La Commission établit un rapport annuel global qui ne peut contenir aucune information confidentielle. Ce rapport est discuté à l'occasion d'un débat en séance plénière de la "Tweede Kamer" et peut donner lieu à des échanges de vues approfondis entre la "Tweede Kamer" et les ministres concernés.

Cependant, la Commission des services de renseignement et de sécurité est informée, par les annexes secrètes du rapport, des détails opérationnels qui ne peuvent être rendus publics pour des raisons de sécurité nationale.

17.5. Examen des plaintes

Les personnes qui estiment avoir été injustement traitées par les services de renseignement et de sécurité peuvent s'adresser à la Commission, à l'ombudsman national ou au ministre concerné. Ces trois autorités se concertent au sujet du traitement des plaintes.

DEUXIEME PARTIE

1. LE BVD

1.1. Arrêté de 1996 organisant le BVD

Un arrêté du ministre de l'Intérieur définit l'organisation du BVD.

1.1.1. Le BVD

Le service dépend directement du Secrétaire général.

1.1.2. La mission du BVD

La mission du BVD trouve son fondement dans l'article 8 de la loi sur les services de renseignement et de sécurité (*cf. 1^{ère} partie, point 6*).

1.1.3. La direction du BVD

La direction du BVD est assurée par le chef et son adjoint.

1.1.4. Composition

Le BVD se compose de six directions :

- de directie Strategie en Planning (D1);
- de directie Democratische Rechtsorde (D2);
- de directie Staatsveiligheid (D3);
- de directie Maatschappelijke en Economische Belangen (D4);
- de directie Operationele Informatievergaring (D5);
- de directie Management, Advies en Centrale Faciliteiten (D6);

1.1.5. Subdivision

Chaque direction se répartit ensuite en différentes unités. Nous en reprenons ici quelques exemples pour permettre au lecteur de mieux comprendre les points suivants.

Les directions Ordre démocratique (D2), Sûreté de l'Etat (D3) et Intérêts sociaux et économiques (D4) se composent chacune :

- het Bedrijfsbureau;
- de afdeling Teamleiding;
- de afdeling Onderzoek;
- de afdeling Documentatie- en Informatievoorziening;

- de afdeling Studie en Bewerking;
- de afdeling Beveiligingsadvies.

La direction Collecte d'informations opérationnelles (D5) se compose :

- de Staf;
- de afdeling Techniek;
- de afdeling Operationele Opdrachten;
- de afdeling Open Bronnen Informatie;
- de afdeling Buitenlandse Relaties;
- de afdeling Speciale Opdrachten.

1.2. Le personnel du BVD

Le BVD est constitué d'environ 530 postes.

1.2.1. Services extérieurs

Le BVD ne dispose pas de services extérieurs, comme c'est le cas pour la Sûreté de l'Etat en Belgique. Les services sont centralisés.

1.2.2. Les fonctionnaires de Police et les Gardes-frontières au service du BVD

L'article 18 de la loi sur les services de renseignement et de sécurité donne un fondement légal aux travaux que certains fonctionnaires désignés de la police et des fonctionnaires chargés de la surveillance des frontières effectuent pour le compte du BVD.

Ces travaux représentent un complément nécessaire à la mission du BVD. Pour ce qui concerne l'intervention de fonctionnaires de police et autres pour le compte du BVD, le principe de la stricte séparation entre les différents travaux est scrupuleusement respecté.

L'article susmentionné détermine les responsables pour la désignation des fonctionnaires qui peuvent entrer en ligne de compte pour une intervention.

Si ces fonctionnaires travaillent pour le BVD, c'est le ministre de l'Intérieur qui est responsable de leur intervention.

L'article 20, 2ème alinéa, de la loi prévoit d'ailleurs que lorsque les fonctionnaires susvisés effectuent des travaux pour le compte du BVD, ils n'ont aucune compétence pour rechercher des faits délictueux. L'article 16 de la loi indique également expressément que les règles relatives à la collecte de données à caractère personnel par le BVD leurs sont applicables.

Le système néerlandais permet toutefois à certains policiers désignés à cet effet de travailler également pour le BVD, mais avec une stricte séparation entre ces deux compétences.

Ce système permet apparemment au BVD de ne pas devoir disposer de services extérieurs.

1.3. Budget du BVD

Le budget du BVD s'élevait à 65,9 millions de florins en 1994, soit environ 0,00033 % du budget

global du pays.

Ce budget se divise en trois parties :

- matériel ;
- personnel ;
- dépenses secrètes.

Le Parlement exerce également un contrôle sur ce budget. Le contrôle des dépenses secrètes du BVD est exercé par le président de la "Algemene Rekenkamer" en personne. Il a le droit d'obtenir les renseignements dont il a besoin, mais il est tenu par la loi à une obligation de secret.

1.4. Méthode de travail du BVD

La mission du BVD porte sur la protection de certains intérêts vitaux. Sur la base d'une analyse des risques, on examine si, et dans quelle mesure, une mission est réservée au BVD.

L'analyse porte sur la nature, le sérieux et l'ampleur des risques qui peuvent conduire à nuire aux intérêts vitaux. Dans l'analyse, on procède à une évaluation cohérente des intérêts en cause, de la menace potentielle et de la résistance sociale.

1.4.1. Le travail avec des "Teams"

Une équipe est généralement constituée lorsque, sur base de l'analyse des risques encourus, il convient d'examiner un phénomène de manière plus approfondie.

1.4.2. Composition d'un "Team"

La taille du "Team" dépend de la nature et de l'ampleur de la mission. Il en va de même pour la composition des membres du "Team". Un "team" est généralement composé de différentes catégories de fonctions. La représentation plus ou moins grande d'une catégorie (par ex. analystes, enquêteurs...) dépend du contenu de la mission du "team".

1.4.3. Durée de l'enquête

On détermine également dans quel délai on prévoit que le "team" aura achevé sa mission. Un team est constitué pour une durée maximale de 1 an.

Ensuite, on procède à une évaluation et on lui assigne éventuellement de nouvelles missions. Si la mission est achevée, le "team" est dissout.

1.4.4. Faire partie de plusieurs Teams

La plupart du temps, il arrive que des personnes travaillent simultanément dans deux teams. Toutefois, il est préférable qu'elles ne travaillent pas en même temps dans un trop grand nombre de teams.

Si les priorités changent, il peut également arriver que l'on supprime un team pour permettre à ses membres de remplir une autre mission.

1.4.5. Juristes

Le BVD dispose aussi de juristes, qui font partie de la Première direction (Stratégie et Planning), et qui peuvent être éventuellement adjoints à une équipe ou qui peuvent être, en tout cas, sollicités pour obtenir un conseil.

1.5. La formation des collaborateurs du BVD

1.5.1. Les différents types de formations

- Formation générale qui repose sur l'initiative de l'intéressé lui-même ;
- Sur l'initiative du service, certains perfectionnements donnés par des personnes extérieures, entre autres concernant les nouveaux développements dans leur spécialité ;
- Accompagnement de carrière, à l'occasion de l'évolution du cadre du personnel, organisé par le Ministère de l'Intérieur - également dans le cadre de changements de fonctions ;
- Formation interne.

1.5.2. Formation interne avant 1990

En 1990, le BVD a connu une profonde réorganisation. Cette réorganisation marque le lancement du "Teamconcept".

Jusqu'en 1990, le service disposait de formations internes. On faisait appel à des formateurs de l'extérieur et de terrain.

1.5.3. Formation après 1990

A partir de 1990, on passe à un système tout à fait différent : le "Modulair Opleidingsysteem". Il s'agit véritablement d'un "travail sur mesure".

Le module de départ forme la base et comprend une orientation générale (par ex. : législation, connaissance de l'organisation du BVD..).

Pour certains, cette base, couplée à la pratique, est suffisante. D'autres devront puiser davantage dans la "gamme des modules" selon leur fonction.

Certaines catégories de travailleurs reçoivent, en outre, une formation complémentaire, également dispensée par des personnes de terrain.

1.6. L'utilisation des sources ouvertes

1.6.1. Organisation de cette section

Cette section "Sources ouvertes" a été constituée lors de la réorganisation du BVD.

1.6.2. Sources ouvertes spécifiques

Bibliothèques, journaux, périodiques, programmes TV et radio, banques de données commerciales...

Il est clairement apparu, lors d'une démonstration de ces sources ouvertes, en particulier avec les banques de données commerciales, que l'accès aux informations souhaitées se faisaient avec une extrême rapidité.

1.6.3. Le travail avec des "intermédiaires"

La section "sources ouvertes" travaille avec des intermédiaires. Ces personnes disposent d'une très bonne connaissance des sources ouvertes, elles maîtrisent l'exploitation des ressources des bibliothèques et des banques de données.

1.7. Le contact avec le Ministère public

A ce propos, nous avons déjà fait référence à la loi (*cfr. 1^{ère} partie, point 12*).

Le responsable du BVD a informé le Comité R qu'une concertation est régulièrement organisée avec le ministère public.

En pratique, cette concertation se déroule généralement avec un "Landelijk Officier van Justitie" désigné à cet effet par les Procureurs généraux. Ce "Landelijk Officier van Justitie" est comparable au magistrat national en Belgique.

1.8. Sanctions disciplinaires et compétence des Tribunaux

1.8.1. Sanctions disciplinaires et pénales

Les collaborateurs du BVD sont passibles de sanctions pénales et disciplinaires, comme tous les autres fonctionnaires civils néerlandais.

Ils s'exposent à des poursuites lorsqu'ils commettent une infraction ou abusent de leurs compétences.

1.8.2. Compétence des tribunaux

Les tribunaux néerlandais sont compétents pour les actes civils et pénaux liés aux activités du BVD.

1.9. L'ombudsman national

L'ombudsman est également compétent pour examiner les plaintes introduites par des citoyens qui s'estiment lésés par les activités du BVD.

TROISIEME PARTIE

1. Le MID

Le MID dépend directement du Secrétaire général (ressort de la compétence du SG).

1.1. La mission du MID

La mission du MID trouve son fondement dans l'article 9 de la loi sur les services de renseignement et de sécurité.

1.1.1. La direction du MID

La direction du MID se compose d'un chef et de son adjoint, en même temps chef d'Etat-major.

1.1.2. Composition

Le MID se compose de huit sections et de l'élément d'organisation : le chef d'Etat-major. Les sections sont :

- Afdeling Inlichtingen;
- Afdeling Contra-Inlichtingen en Veiligheid;
- Afdeling Beleid, Plannen en Controle;
- Afdeling Verbindingsinlichtingen;
- Afdeling Operaties;
- Afdeling Militaire Inlichtingendienst bij de Koninklijke Marine;
- Afdeling Militaire Inlichtingendienst bij de Koninklijke Landmacht;
- Afdeling Militaire Inlichtingendienst bij de Koninklijke Luchtmacht.

1.1.3. Subdivision

Certaines sections comprennent plusieurs éléments d'organisation. Nous en citons quelques exemples, qui permettront aux lecteurs de mieux comprendre les points suivants :

La section "Renseignement" comprend les éléments d'organisation suivants :

- Bureau Strategische Analyse;
- Bureau Militaire Aangelegenheden.

La section "Contre-espionnage et Sécurité" comprend les éléments d'organisation suivants :

- Bureau Contra-Inlichtingen;
- Bureau Veiligheidsonderzoeken;
- Bureau Industrieveiligheid;
- Bureau Militaire Inlichtingendienst- Detachement.

1.2. Personnel du MID

Le MID dispose actuellement de 872 postes.

1.3. Budget du MID

Le contrôle des dépenses secrètes du MID est exercé par le président de la Cour des Comptes en personne. Il a le droit d'obtenir les renseignements dont il a besoin, mais il est tenu par la loi à une obligation de secret.

1.4. Méthode de travail du MID

L'organisation du MID est conçue de telle manière que chaque section se voit attribuer une mission bien définie, généralement remplie par les bureaux appartenant à la section.

La mission du MID porte, d'une part, sur la collecte de données relatives au potentiel et aux forces armées d'autres puissances. Les données recueillies servent à réaliser une évaluation correcte afin de déterminer la structure et l'utilisation des forces armées des Pays-Bas.

D'autre part, des données sont recueillies et des analyses de risques réalisées pour les régions où l'armée néerlandaise est présente, peut être présente ou sera présente dans le cadre d'opérations de maintien de la paix, de gestion de crises ou d'opérations à caractère humanitaire, sous les auspices de l'ONU, de l'OTAN, de l'UEO, etc.

Par ailleurs, des informations sont également recueillies à propos de menaces (potentielles) qui visent les forces armées. Il s'agit ici de risques qui peuvent nuire aux intérêts de la défense, comme la sécurité, et à la capacité d'intervention des forces armées. Sur la base d'une analyse de risques qui évalue la nature, le sérieux et l'ampleur du risque en relation avec les intérêts de défense en cause, des mesures de protection peuvent être conseillées et adoptées. De plus, des enquêtes de sûreté sont menées sur des (candidats) fonctionnaires de confiance à la Défense.

1.5. La formation des collaborateurs du MID

1.5.1. Différents types de formations

Formation générale qui repose sur l'initiative de l'intéressé lui-même.

1.5.2. Formation avant 1987

Jusqu'en 1987, il existait trois services de renseignement militaires, à savoir :

- le Service de Renseignements de la Marine ;
- le Service de Renseignements des Forces terrestres;
- le Service de Renseignements de la Force aérienne.

Jusqu'à cette période, les formations étaient essentiellement assurées par la force militaire concernée et, dans certains cas, une formation de base et de perfectionnement était suivie au BVD.

1.5.3. Formation après 1987

La formation après 1987 : lors de l'adoption de la loi sur les services de renseignement et de sécurité (1987), les trois services de renseignement militaires ont été intégrés pour former le MID.

Une formation spécifique des collaborateurs du MID, de la compétence du Contre-espionnage et de la Sûreté, est assurée par l'école du MID (SMID) des Forces terrestres.

C'est là que le système de formation modulaire a été introduit. Chaque collaborateur concerné du MID suit, en principe, le "cours de base".

Le cours de base est une orientation générale qui focalise son attention, entre autres, sur l'organisation du MID, les principes élémentaires du travail de Renseignement (en particulier le Contre-espionnage) et de Sûreté ainsi que sur la loi et la réglementation.

Pour certains, ce cours de base est suffisant. D'autres devront suivre des cours complémentaires, en dehors de la défense également, selon la fonction qu'ils doivent exercer. D'autre part, certains collaborateurs suivent des cours spécialisés à l'étranger.

Les nouveaux collaborateurs du MID suivent un cours spécifique consacré à l'organisation, aux missions et à la méthode de travail du MID.

1.6. Le contact avec le Ministère public

A ce propos, nous avons déjà fait référence à la loi (*cf. 1^{ère} partie, point 12*).

1.7. Sanctions disciplinaires et compétence des tribunaux

1.7.1. Sanctions disciplinaires et pénales

Les collaborateurs du MID sont passibles de sanctions pénales et disciplinaires, comme tous les autres fonctionnaires civils néerlandais.

Ils s'exposent à des poursuites lorsqu'ils commettent une infraction ou abusent de leurs compétences.

1.7.2. Compétence des Tribunaux

Les tribunaux néerlandais sont compétents pour les actes civils et pénaux liés aux activités du MID.

1.8. L'ombudsman national

L'ombudsman est également compétent pour examiner les plaintes introduites par des citoyens qui

s'estiment lésés par les activités du MID.

1.9. Collaboration entre le MID et le BVD

Le MID et le BVD travaillent en étroite collaboration lorsque leurs sphères de compétences se recoupent.

Cette collaboration est définie dans les grandes lignes dans une convention de collaboration BVD - MID établie par les ministres concernés.

QUATRIEME PARTIE

APPROCHE CRITIQUE

1. La base légale

Comme nous l'avons déjà indiqué plus haut, les Pays-Bas disposent, tout comme la Belgique, de deux services de renseignement, à savoir : le BVD et le MID, placés sous la responsabilité respective du ministère de l'Intérieur et du ministère de la Défense.

Ces services disposent d'une base légale, à savoir la loi du 3 décembre 1987 sur les services de renseignement et de sécurité.

Cette loi indique explicitement que pour l'organisation, la méthode de travail et la gestion d'un service, seul le ministre responsable du service peut en préciser les règles. Ce ministre est politiquement responsable devant le Parlement.

Cette disposition diverge de la disposition du projet de loi belge du 20 juin 1996 sur les services de renseignement et de sécurité, qui accorde au ministre de l'Intérieur un droit de cogestion important dans la gestion de la Sûreté de l'Etat.

A cet égard, le Comité R se pose la question de savoir si une procédure aussi lourde ne risque pas d'avoir des conséquences sur le bon fonctionnement du service et la responsabilité politique de chaque ministre.

Aux Pays-Bas, il existe, déjà depuis 1976, une "Commission ministérielle pour les services de renseignement et de sûreté".

Par arrêté royal du 21 juin 1996, un "Comité ministériel pour le Renseignement et la Sûreté" a été constitué en Belgique, avec pour mission, tout comme aux Pays-Bas :

"(...) de définir la politique générale en matière de renseignement (définir les priorités de la Sûreté de l'Etat et du Service général de Renseignement et de Sûreté des forces armées) et de coordonner leurs activités".

Pour la composition de ce Comité ministériel, on retrouve également de grandes ressemblances avec les Pays-Bas. Dans les deux pays, cet organe est présidé par le Premier ministre et l'on y retrouve, entre autres, les ministres de la Justice, de la Défense, de l'Intérieur et des Affaires étrangères.

L'arrêté royal du 21 juin 1996, a constitué le Collège pour le Renseignement et la Sécurité, comparable au "Comité Verenigde Inlichtingendiensten Nederland".

En Belgique, ce Collège, comme aux Pays-Bas, est composé des responsables des services de renseignement et des hauts fonctionnaires des Ministères des Affaires étrangères, et de l'Intérieur, pour la Belgique, et de la Justice, pour les Pays-Bas.

Le législateur au Pays-Bas a créé la fonction de coordinateur en lui conférant un rôle important. Il

s'agit là d'une différence entre les Pays-Bas et la Belgique qui n'a pas envisagé la mise en place de cette autorité.

Le Comité R regrette quelque peu que l'on n'ait accordé aucune attention à cette fonction pendant les travaux préparatoires du projet de loi sur les services de renseignement et de sécurité ⁽¹⁾.

2. Faut-il une législation exhaustive sur les services de renseignement ?

Dans la loi néerlandaise du 3 décembre 1987 sur les services de renseignement et de sécurité, les missions du BVD et du MID sont décrites de manière plutôt succincte.

Dans le projet de loi belge, le gouvernement a tenu compte des remarques du Conseil d'Etat. Ainsi le contenu des menaces, auxquelles les services de renseignement s'intéressent, a été défini.

Le Comité R estime qu'en se faisant, il a été tenu compte des droits que la Constitution et les lois confèrent aux citoyens et du fait que la mission des services de renseignement se trouvera facilitée par une description précise des menaces.

En ce qui concerne la méthode de travail des services de renseignement néerlandais, leur législation est très sommaire.

En résumé, la loi néerlandaise stipule que la mission de ces fonctionnaires consiste à recueillir, enregistrer et analyser des informations, émanant aussi bien de sources ouvertes que de sources fermées, et à collaborer entre services et avec les services alliés étrangers, avec pour objectif d'informer à temps les autorités compétentes de menaces éventuelles qui pèsent sur la sécurité ou d'autres intérêts vitaux de l'Etat. Le législateur a conféré la même mission au MID en précisant qu'elle portait sur le potentiel des forces armées d'autres puissances et de leur sécurité.

La loi prévoit que seul le BVD peut écouter des conversations téléphoniques, les enregistrer et écouter, à l'aide d'appareils, des conversations dans des habitations, des locaux fermés ou ailleurs. En outre, ce service peut capter des données transmises par ordinateur. Cette compétence est toutefois réglée par le Code pénal néerlandais.

Par ailleurs, d'autres méthodes sont utilisées pour recueillir des informations, par exemple la filature et l'observation de personnes. Le recours à ces méthodes est légitimé par la mission que leur confère la loi.

Aux Pays-Bas, la révision de la loi de 1987 sur les services de renseignement et de sécurité est en cours de discussion, suite à l'arrêt rendu par le Conseil d'Etat dans les causes Van Baggum et Valkenier c/ ministre de l'Intérieur.

Cette modification de la loi implique que, certaines méthodes comme la filature et l'observation, avec ou sans appareillages d'observation ou de localisation seront clairement définies dans le projet de loi.

Dans son avis relatif à l'avant-projet de loi belge sur les services de renseignement et de sécurité, le Conseil d'Etat a fait observer, à juste titre, que l'on accordait trop peu d'attention aux méthodes que les services de renseignement pouvaient utiliser pour recueillir leurs informations. A cet égard, la jurisprudence de la Cour européenne des droits de l'homme n'est pas respectée.

Le Comité R estime que l'utilisation de certaines méthodes par les services de renseignement,

⁽¹⁾ Voir rapport annuel 1995 du Comité R, chapitre 3, pp. 65 à 67

comme l'interception de courrier, l'observation, avec ou sans utilisation d'appareillages, sont des moyens de contrainte et doivent donc être régis par la loi. A cet égard, le Comité R regrette qu'il n'ait pas été tenu compte de l'avis du Conseil d'Etat lors de la rédaction du projet de loi ⁽¹⁾.

Aux Pays-Bas par contre, les méthodes que pourront utiliser les services de renseignement seront réglées par la loi.

La disposition selon laquelle les fonctionnaires des services ne seront pas compétents pour rechercher des faits délictueux est importante.

Cette différence de compétences entre les services de renseignement et les services de police se retrouve dans notre pays et dans bien d'autres, comme le Portugal, le Canada, l'Allemagne...

Ce choix peut s'expliquer par les objectifs différents que poursuivent un service de renseignement et un service de police et afin d'éviter une trop forte concentration de pouvoir au sein d'un même service.

Toutefois, la législation néerlandaise prévoit que, certains fonctionnaires de police et fonctionnaires chargés de la surveillance des frontières, peuvent accomplir des missions pour le BVD.

Ils partent du principe que ces activités représentent un complément nécessaire à la mission du BVD. Dans cette hypothèse de travail, ces fonctionnaires n'ont plus de compétence pour rechercher des infractions et sont placés sous la responsabilité du ministre de l'Intérieur.

Il ressort cependant des travaux préparatoires de la loi de 1987 que ce choix a été opéré en vue d'éviter un élargissement considérable des effectifs des services.

A cet égard, on peut se poser la question suivante : le transfert de compétences de renseignements à des fonctionnaires de police ne risque-t-il pas de créer une confusion entre les différentes fonctions et responsabilités de chacun des services, malgré les mesures de précaution prises dans la loi pour assurer une différenciation des compétences ?

3. Un service de renseignement spécifique compétent pour l'étranger ?

Jusqu'au 1^{er} janvier 1994, les Pays-Bas disposaient de l'IDB (Service de Renseignement Etranger). La suppression de ce service, a mis fin à certaines activités.

D'autres activités de l'IDB, décrites par la loi dans les missions légales du MID et du BVD, ont été reprises par ces services.

A ce sujet, le Comité R ne peut que se féliciter de l'initiative du législateur belge qui fixe les circonstances dans lesquelles les services de renseignement belges seront également compétents pour exercer des activités à l'étranger.

En raison de la situation géographique et démographique des deux pays, le Comité R estime qu'un service de renseignement spécifique pour l'étranger n'est pas indispensable. Cette mission ne peut toutefois être négligée par les services actuels.

⁽¹⁾ Voir titre II - première partie - chapitre 1 ("Audition des membres du Comité R devant les Commissions réunies de la justice et de la Défense nationale le 7 janvier 1997").

Le projet de loi belge en tient compte.

4. *La coordination et la collaboration entre les services de renseignement - la collaboration entre le Ministère public et la police, d'une part, et les services, d'autre part, la collaboration avec les services de renseignement étrangers.*

La loi prévoit que les responsables des services apportent tout leur concours au coordinateur pour l'exercice de sa fonction. Ils sont tenus de lui fournir toutes les informations nécessaires à cet effet.

Dans la perspective de cette disposition, la loi prévoit également que les services doivent autant que possible collaborer, notamment en échangeant des informations qu'ils détiennent.

Les travaux préparatoires de la loi exposent qu'en ce qui concerne des informations détenues par d'autres pouvoirs publics, il est indispensable que le MID se consulte avec le responsable du BVD, afin d'éviter que le même travail soit effectué à deux reprises.

Le MID et le BVD collaborent dans leurs sphères de compétences respectives qui se chevauchent.

Cette collaboration est fixée dans les grandes lignes dans un accord de collaboration BVD - MID établi par les ministres concernés.

En ce qui concerne la coopération des services néerlandais avec les services de renseignement étrangers, la loi prévoit que les responsables des services veillent à entretenir des liens avec les services de renseignement et de sécurité d'autres puissances concernées. La collaboration des services de renseignement avec le Ministère public et les services de police est définie dans la loi et une concertation régulière est prévue entre le Ministère public et les services de renseignement.

Le projet de loi belge n'aborde que sommairement cette problématique en indiquant que les services de renseignement et de sécurité veillent à une collaboration parfaite et que, à la demande de la Sûreté de l'Etat ou du Service général de Renseignement et de Sécurité, il apporte sa collaboration pour la collecte de renseignements si des militaires sont concernés par certaines activités. A l'inverse, lorsque des civils sont concernés dans le cadre de missions effectuées par le SGR, c'est la Sûreté de l'Etat qui recueillera des informations.

En ce qui concerne la collaboration avec les autorités judiciaires, les services de police et les services de renseignement étrangers, le projet de loi belge mentionne dans un paragraphe, en son chapitre intitulé "L'exercice des missions" : "*(...) Ces renseignements ne peuvent être communiqués qu'aux ministres et aux autorités judiciaires et administratives concernés, aux services de renseignement et de sécurité et aux services de police qui en ont besoin pour l'exécution de leurs missions*".

Il ressort des travaux préparatoires que l'on vise ici l'échange d'informations, tant entre les services de renseignement belges qu'étrangers.

Le Comité R estime que ce règlement est beaucoup trop succinct et propose la solution adoptée par la législation néerlandaise et allemande⁽¹⁾.

Le Comité R se réjouit de la rédaction intervenue depuis février 1997, d'un protocole d'accord portant sur la coordination et la collaboration entre le SGR et la Sûreté de l'Etat et de son

⁽¹⁾ Voir rapport annuel 1996 du Comité R "Allemagne" - p. 10 "La collaboration"

approbation par les ministres compétents.

Il n'en demeure pas moins que le Comité R estime que la loi devrait préciser le contenu de la collaboration entre les services belges⁽¹⁾.

5. Les enquêtes de sécurité

Aux Pays-Bas, les services de renseignement mènent les enquêtes de sécurité sur l'exercice de fonctions de confiance, de fonctions dans le monde économique, etc.

La loi définit les principes qui permettent d'identifier des fonctions de confiance, à savoir :

- pouvoir prendre connaissance de données liées à des secrets d'Etat ;
- réaliser des travaux relatifs à des secteurs des pouvoirs publics et du monde économique qui sont d'un intérêt vital pour la défense du pays ou pour le maintien de la vie en société.

Depuis le 1^{er} février 1997, la loi sur les enquêtes de sécurité est en vigueur aux Pays-Bas (loi du 10 octobre 1996). Auparavant, il n'existait aucune réglementation uniforme pour l'ouverture d'enquêtes de sécurité.

Il existe actuellement en Belgique un avant-projet de loi relatif aux habilitations en matière de sécurité.

Le Comité R estime utile de fixer certains critères, sur le modèle néerlandais, pour désigner les fonctions (tant dans le secteur public que privé) où une habilitation en matière de sécurité est nécessaire.

Le Comité R se réjouit également de l'avant-projet de loi qui l'instaure en tant qu'instance d'appel pour la délivrance des habilitations en matière de sécurité.

Aux Pays-Bas, il existe une procédure de réclamation auprès de l'organisme public qui a pris la décision et une possibilité d'appel auprès du juge administratif, avec une possibilité d'appel. Cette procédure n'est pas prévue dans la loi sur les enquêtes de sécurité, mais se fonde sur la loi dénommée "Algemene Wet Bestuursrecht".

6. La collecte de données à caractère personnel par les services

La loi "wet Persoonsregistraties", en vigueur pour la collecte de données à caractère personnel par les pouvoirs publics et les entreprises privées, ne s'applique pas aux recueils de données à caractère personnel conservées par ou au bénéfice des services de renseignement et de sécurité⁽¹⁾.

Ces recueils de données sont réglés par la loi sur les services de renseignement et de sécurité.

Dans cette loi, toute une procédure est prévue pour la consultation et la gestion de collectes de

⁽¹⁾ Voir titre II - première partie - chapitre 1 ("*Audition des membres du Comité R devant les Commissions réunies de la justice et de la Défense nationale le 7 janvier 1997*").

⁽²⁾ A comparer avec la loi belge du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

données à caractère personnel.

La communication de données à caractère personnel aux services par un organisme public ou une entreprise est réglée par la loi.

Comme en Belgique, la règle de la finalité s'applique ici, à savoir que les services ne peuvent recueillir et conserver des données à caractère personnel que dans la mesure où cela est nécessaire pour l'exécution des missions décrites dans la loi.

Dans le projet de loi belge, on retrouve cependant une réglementation très sommaire pour la collecte de données à caractère personnel, à savoir :

Art. 10 § 2

(...)

"Dans le cadre de leurs missions, ils peuvent rechercher, collecter et recevoir des données à caractère personnel et des informations relatives à des événements, à des personnes et à des groupes, qui peuvent être utiles à l'exécution de leurs missions."

Art. 10 § 3

" Dans l'exercice des missions qui leurs sont confiées, ils peuvent traiter ces données et ces informations et tenir à jour une documentation, relative notamment à des événements, à des groupements et à des personnes présentant un intérêt pour l'exécution de leurs missions".

A cet égard, le Comité R s'associe entièrement aux remarques formulées par le Conseil d'Etat, à savoir : "(...) que le projet de loi ne contient aucune règle claire et détaillée concernant la collecte et l'utilisation de renseignements, (...)", et, par conséquent, n'est pas conforme, à l'article 8, 2ème alinéa de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales.

Le Comité R recommande de tenir compte des remarques du Conseil d'Etat et de fixer des règles claires pour la collecte et la conservation de données à caractère personnel.

7. Droit de consultation d'un particulier

Comme nous l'avons indiqué plus haut, la loi néerlandaise sur les services de renseignement et de sécurité stipule que l'on ne peut accorder, en général, à des particuliers un droit de consultation des données détenues par un service.

La section administrative du Conseil d'Etat a déclaré que cet article, qui règle, entre autres, la publicité des données à caractère personnel dans les dossiers de renseignements et de sécurité, est contraire aux articles 8 et 13 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales.

Cette décision a provoqué l'élaboration d'un texte modifiant la loi sur les services de renseignement et de sécurité.

A propos de cette problématique le Comité R renvoie le lecteur au rapport concernant l'accès aux dossiers des services de renseignement par un particulier ⁽¹⁾.

⁽¹⁾ Voir titre II - première partie - chapitre 2 du présent rapport.

8. Restrictions au droit fondamental de quitter librement le territoire

Cette restriction est reprise dans la loi néerlandaise sur les services de renseignement et de sécurité. Cette disposition (qui prévoit des exceptions) offre une protection supplémentaire, tant pour les fonctionnaires des services que pour leurs informateurs. Le Comité R recommande que le législateur belge envisage d'insérer dans la loi sur les services de renseignement une disposition semblable.

9. Obligation de secret

Le Comité R souhaite attirer une fois encore l'attention du législateur belge sur la réglementation prévue dans la législation néerlandaise qui concerne l'hypothèse où un fonctionnaire est convoqué comme témoin ou expert.

Ce fonctionnaire ne peut faire de déclaration sur des éléments couverts par son devoir de confidentialité que si le ministre compétent et le ministre de la Justice l'ont conjointement déchargé de cette obligation par écrit.

Le Comité R a ouvert, à ce sujet, une enquête de contrôle le 15 mai 1997.

10. La formation des fonctionnaires des services de renseignement et de sécurité

Comme indiqué dans le corps du texte de ce rapport, les deux services de renseignement néerlandais ont accordé beaucoup d'attention à la formation de leurs collaborateurs.

Il semble tout à fait opportun d'envisager pour les services belges, Sûreté de l'Etat et SGR, un système de formation modulaire semblable à celui en vigueur au BVD et au MID. Le Comité R recommande une formation conjointe des agents des services de renseignement à tout le moins relative à leur formation générale.

11. L'établissement d'un rapport annuel

Le Comité R recommande que les services belges envisagent, sur le modèle néerlandais, de rédiger un rapport annuel public, ce qui donnerait une plus grande transparence des activités de ces services à l'égard du public.

12. Utilisation des sources ouvertes

Le Comité R recommande d'accorder à l'avenir plus d'attention à une utilisation optimale des sources ouvertes. Une utilisation efficace de ces sources est de nature à faire gagner du temps et à économiser des moyens.

Il convient de souligner que les services belges déclarent eux-mêmes que 80% de leurs informations proviennent de sources ouvertes. L'intérêt d'utiliser ces sources d'une manière plus appropriée et plus efficace apparaît donc pour tous les protagonistes du renseignement.

13. Le contrôle parlementaire sur les services de renseignement et de sécurité

Dès 1952, les Pays-Bas ont constitué une "Vaste Commissie voor de Inlichtingen- en Veiligheidsdiensten". Cette Commission se compose actuellement des présidents de groupe des quatre principaux partis politiques. Une concertation régulière entre les présidents de groupe et les ministres responsables des services a conduit à une pratique où presque tous les aspects de la mission des services, leur organisation et leur méthode de travail font ou peuvent faire l'objet de discussions.

Cette Commission est informée des opérations menées par les services de renseignement.

La Commission établit un rapport annuel global qui ne peut contenir aucune information confidentielle. Ce rapport est discuté à l'occasion d'un débat en séance plénière de la "Tweede Kamer" et peut donner lieu à des échanges de vues approfondis entre la "Tweede Kamer" et les ministres concernés.

Bien que les Pays-Bas aient toujours accordé beaucoup d'attention à un contrôle parlementaire sur les services de renseignement, on peut noter à juste titre à cet égard que le législateur belge, en créant le Comité permanent de contrôle des services de renseignement, a permis au parlement d'exercer ce contrôle de manière efficace tout en respectant l'avis donné par le Conseil d'Etat en la matière.

La charge de travail des présidents des quatre principaux partis est sans conteste une lourde charge. On peut se poser, dès lors, la question de leur disponibilité pour ajouter au travail législatif cette mission de contrôle.

Par contre, le Comité R est un organe permanent. Il dispose d'un Service d'enquêtes et d'une série de moyens de contrainte qui permettent un contrôle efficace. Les enquêteurs ont accès aux locaux où les services de renseignement effectuent leurs travaux et peuvent également procéder à des saisies.

Néanmoins, des garde-fous ont été mis en place en vue d'éviter que la vie ou l'intégrité physique de particuliers soit mise en danger par des actes d'enquêtes.

Le règlement d'ordre intérieur prévoit, des mesures de précaution notamment en ce qui concerne la protection des informateurs et des informations émanant des services de renseignement étrangers.

Le Comité R estime que la législation belge est un bon exemple en la matière et espère également qu'à l'avenir, tout comme aux Pays-Bas, son rapport d'activités annuel fera l'objet d'échanges de vues entre les membres du Parlement et les ministres compétents.

Le Conseil d'Etat belge a fait remarquer, en outre, que la constitution d'une Commission parlementaire permanente de contrôle des services de police et de renseignement se heurte à quelques objections au point de vue de sa constitutionnalité ⁽¹⁾.

⁽¹⁾ Avis du Conseil d'Etat sur la proposition de loi pour la constitution d'une commission parlementaire permanente de contrôle des services de police, de la gendarmerie et le département "Sûreté de l'Etat" de l'administration de la sûreté publique du Ministère de la Justice (Chambre des Représentants - 162/2 - 1988).

TITRE II : NOS SERVICES DE RENSEIGNEMENT

PREMIERE PARTIE : LES ETUDES

CHAPITRE 1 : AUDITION DES MEMBRES DU COMITÉ R DEVANT LES COMMISSIONS RÉUNIES DE LA JUSTICE ET DE LA DÉFENSE NATIONALE LE 7 JANVIER 1997

INTRODUCTION

Le 7 janvier 1997, le Comité R a été invité à donner son avis sur le projet de loi organique des services de renseignement et de sécurité (document parlementaire, la Chambre, session 1995-1996, n°638/1-1995-1996) devant les commissions réunies de la Justice et de la Défense nationale.

Dans son rapport général d'activités 1995, deux membres avaient analysé la note d'orientation gouvernementale sur les services de renseignement ⁽¹⁾.

Le Comité R a examiné, chapitre par chapitre, le projet de loi pour donner son avis.

CHAPITRE 1er : Dispositions générales

Article 2

“La présente loi s’applique à la Sûreté de l’Etat, service civil de renseignement et de sécurité, et au Service général du renseignement et de la sécurité des Forces armées, service militaire de renseignement et de sécurité, qui sont les deux services de renseignement et de sécurité du Royaume.”

Le projet de loi ne vise que la Sûreté de l’Etat et le SGR.

L’exposé des motifs précise : *“il s’agit d’éviter qu’en dehors du contexte d’une loi, des services de renseignement et de sécurité parallèles puissent être constitués”*. ⁽¹⁾

D’autres services, notamment les services de police, exécutent des missions de renseignement et ce en vertu de la loi. En effet, l’article 39 de la loi du 5 août 1992 sur la fonction de police autorise les services de police à faire du renseignement. Cet article prévoit :

“Dans l’exercice des missions qui leur sont confiées les services de police peuvent recueillir des informations, traiter des données à caractère personnel et tenir à jour une documentation relative

⁽¹⁾ Comité R - Rapport d’activités 1995 - p.60

⁽²⁾ Doc. Parl., 638 / 1-95 / 96, p. 7

notamment à des événements, à des groupements et à des personnes présentant un intérêt concret pour l'exécution de leurs missions de police administrative ou judiciaire.

Les renseignements contenus dans la documentation doivent présenter un lien direct avec la finalité du fichier et se limiter aux exigences qui en découlent.

Ces renseignements ne peuvent être communiqués qu'aux autorités et services de police ainsi qu'aux services de renseignement officiels qui en ont besoin pour l'exécution de leurs missions."

La gendarmerie fait partie du collège du renseignement et de la sécurité institué par arrêté royal du 21 juin 1996, (Moniteur belge du 5 septembre 1996 - article 2). Il paraît surprenant qu'un service de police ait une voix dans un collège destiné à veiller à la coordination opérationnelle des services de renseignement. Dans le projet de loi les corps de police ne sont pas soumis aux mêmes obligations et droits que la Sûreté de l'Etat et le SGR en ce qui concerne leurs missions de renseignement.

La gendarmerie fait du renseignement à l'occasion du maintien de l'ordre et de la sécurité comme en atteste son livre II qui est relatif à ses directives internes.

Un protocole d'accord est en cours d'élaboration entre la Sûreté de l'Etat et la gendarmerie. Ce fait démontre à suffisance que les actions de ces deux services se chevauchent notamment à l'occasion des missions de police proactive exercées par la gendarmerie.

La police judiciaire et la police communale font également du renseignement. Il en est ainsi, par exemple, en ce qui concerne le suivi des activités des sectes nuisibles.

Deux membres se réfèrent à cet égard au rapport annuel d'activités 1995 du Comité R qui précise à la page 88 :

"La future loi sur les services de renseignement devra viser, non seulement la Sûreté de l'Etat et le SGR, mais aussi tous les autres services (police, gendarmerie, etc...). Dans la mesure où ils sont habilités à recueillir, traiter et analyser des renseignements de sécurité."

Dans cette optique et pour les raisons développées ci-dessus, le Comité R propose au parlement d'ajouter un deuxième alinéa à l'article 2 de la future loi qui pourrait être rédigé comme suit :

"Aucun autre service ne peut exécuter des missions de renseignement et de sécurité qu'en vertu d'une loi."

CHAPITRE II : L'organisation et les missions

Comme le fait à juste titre remarquer le Conseil d'Etat (p. 30 du document parlementaire précité) *"l'organisation des services administratifs de l'Etat constitue en vertu des articles 37 et 107, alinéa 2, de la Constitution, une prérogative du pouvoir exécutif"*.

Ce chapitre devrait donc uniquement porter sur les missions des services de renseignement et non sur l'organisation et les missions.

Le Comité R estime, en outre, qu'il n'est pas souhaitable que ces deux aspects de la loi soient repris dans un seul chapitre pour des raisons évidentes de clarté.

Article 4

Le deuxième alinéa de cet article dispose :

“Dans l’exercice de ses missions, la Sûreté de l’Etat veille au respect et contribue à la protection des libertés et droits individuels, ainsi qu’au développement démocratique de la société.”

Ce texte concerne une obligation générale pour la Sûreté de l’Etat.

Le Comité R propose deux solutions à ce propos :

1. cet alinéa pourrait chapeauter les articles 7 et 9 relatifs respectivement aux missions de la Sûreté de l’Etat et du Service général du renseignement et de la sécurité ;
2. cet alinéa pourrait faire l’objet d’un article unique à placer dans le chapitre I de la loi concernant les dispositions générales.

Articles 5 et 6

“Article 5 :

§ 1^{er} Pour l’exécution de ses missions, la Sûreté de l’Etat est placée sous l’autorité du ministre de la Justice.

§ 2 Toutefois, le ministre de l’Intérieur peut requérir la Sûreté de l’Etat pour ce qui concerne l’exécution des missions prévues à l’article 7, § 1^{er}, lorsqu’elles ont trait au maintien de l’ordre public et à la protection des personnes.

Dans ce cas, le ministre de l’Intérieur, sans s’immiscer dans l’organisation du service, précise l’objet de la réquisition et peut faire des recommandations et donner des indications précises sur les moyens à mettre en oeuvre et les ressources à utiliser.

Lorsqu’il est impossible de se conformer à ces recommandations et indications parce que leur exécution porterait atteinte à l’exécution d’autres missions, le ministre de l’Intérieur en est informé dans les meilleurs délais. Cela ne dispense pas la Sûreté de l’Etat de l’obligation d’exécuter les réquisitions qui ont trait à la protection des personnes.

§ 3 Le ministre de la Justice est chargé de l’organisation et de l’administration générale de la Sûreté de l’Etat, en particulier en ce qui concerne les dépenses, l’administration du personnel et la formation, l’ordre intérieur et la discipline, les traitements et indemnités, ainsi que l’équipement.

Article 6 :

§ 1^{er} Le ministre de l’Intérieur est associé à l’organisation et à l’administration de la Sûreté de l’Etat, conformément aux §§ 2, 3 et 4, lorsque celles-ci ont une influence directe sur l’exécution des missions de maintien de l’ordre public et de protection des personnes.

Si le ministre de la Justice estime ne pas pouvoir donner suite à une demande du ministre de l’Intérieur, il informe ce dernier de ses raisons.

§ 2. La signature conjointe du ministre de l’Intérieur est requise pour :

1° tout projet de loi relatif à la Sûreté de l’Etat;

2° tout projet d'arrêté réglementaire relatif à l'organisation générale de la Sûreté de l'Etat.

§ 3. L'avis conforme du ministre de l'Intérieur est requis pour :

- 1° tout projet d'arrêté relatif au cadre organique du personnel de la Sûreté de l'Etat;
- 2° tout projet d'arrêté royal relatif à la nomination et à l'affectation des fonctionnaires généraux de la Sûreté de l'Etat;
- 3° tout projet d'arrêté réglementaire relatif aux délégations spécifiques en matière budgétaire;
- 4° tout projet d'arrêté déterminant la formation du personnel des Services extérieurs qui concerne les missions pour lesquelles la Sûreté de l'Etat peut faire l'objet d'une réquisition en matière de protection des personnes;
- 5° tout projet d'arrêté fixant le nombre d'agents des Services extérieurs de la Sûreté de l'Etat qui seront désignés comme officiers de protection et désignant l'officier qui en a la charge;
- 6° l'avant-projet du budget concernant la Sûreté de l'Etat;
- 7° tout projet d'arrêté réglementaire relatif aux attributions spécifiques du fonctionnaire qui dirige la Sûreté de l'Etat.

Le ministre de l'Intérieur donne son avis dans le délai fixé par le ministre de la Justice, ce délai ne pouvant être inférieur à vingt jours ouvrables. En cas d'urgence motivée, ce délai peut être ramené à cinq jours ouvrables. Passé ces délais, l'avis est réputé conforme. L'avis non conforme est motivé.

§ 4. *Le Roi détermine les matières relatives à l'organisation et à l'administration de la Sûreté de l'Etat, autres que celles visées aux §§ 2 et 3, et qui ont une influence directe sur l'exécution des missions de maintien de l'ordre public et de protection des personnes, pour lesquelles le ministre de la Justice demande un avis au ministre de l'Intérieur ou l'informe, ainsi que les modalités s'y rapportant.*"

Comme indiqué ci-dessus, le Comité R estime qu'il faut tenir compte de l'avis du Conseil d'Etat à ce sujet.

"Il importe de rappeler l'organisation des services administratifs de l'Etat constitue, en vertu des articles 37 et 109 - alinéa 2 de la Constitution, une prérogative du pouvoir exécutif"⁽¹⁾.

Si le parlement devait passer outre l'avis du Conseil d'Etat, les mêmes deux membres se réfèrent au rapport annuel d'activités du Comité R 1995, p. 89 :

"Nous ne pouvons marquer notre accord avec les prérogatives reconnues aux deux ministres précités (ministre de l'Intérieur et ministre des Affaires étrangères), à savoir formuler des recommandations et donner des indications sur les moyens à mettre en oeuvre et les ressources (ou sources) à utiliser. De telles prérogatives sont de nature à engendrer des conflits d'autorité et des frustrations entre les ministres et les services de renseignement. Nous sommes plutôt d'avis que ce pouvoir de recommandation sur les moyens à mettre en oeuvre devrait être réservé au coordinateur dont il a été question plus haut. En tout état de cause, nous estimons que ces recommandations devront rester secrètes à l'égard du public.

Selon nous, le droit de réquisition accordé au ministre de l'Intérieur ne justifie pas davantage qu'il

⁽¹⁾ Doc. parl. - 638/1 - 95-96 p. 30

soit associé à la gestion de la Sûreté de l'Etat, notamment en intervenant dans les actes d'administration de ce service."

De plus, ces deux membres ne voient pas pourquoi le ministre de l'Intérieur aurait plus de droit que le ministre des Affaires étrangères ou qu'un autre ministre (ministre des Affaires économiques, par exemple), alors que l'article 7 relatif aux missions de la Sûreté de l'Etat prévoit également que ce service veillera à la sûreté extérieure de l'Etat, aux relations internationales et au potentiel scientifique ou économique du pays.

Ces deux membres du Comité R soumettent à la réflexion du parlement une autre solution, dans la mesure où cette commission désire une autre ouverture que celle proposée par le gouvernement.

Cette piste de réflexion est de nature à pallier aux inconvénients que nous avons décrits dans le rapport annuel d'activités de 1995. Elle consiste à mettre l'entière responsabilité de l'organisation de la Sûreté de l'Etat à charge du ministre de l'Intérieur.

Tout d'abord, l'histoire des services de renseignement nous apprend que la Sûreté de l'Etat a été rattachée au ministre de l'Intérieur dans la seconde moitié du 19^{ème} siècle.

Ensuite, les articles du projet de loi ne visent en aucun cas des activités relevant de la responsabilité ministérielle du ministre de la Justice. La Justice et le Renseignement sont deux matières distinctes l'une de l'autre.

Enfin, aucune loi des pays étudiés jusqu'à présent par le Comité R ne donne cette responsabilité au ministre de la Justice.

Un membre du Comité R estime que la détermination des ministres compétents en cette matière est une question politique. A ce sujet, ce membre ne désire pas prendre position.

Article 7 : les missions de la Sûreté de l'Etat

1. l'article 7 § 1^{er} 1^o :

"la Sûreté de l'Etat a pour mission de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure de l'Etat et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'Etat et les relations internationales, ou le potentiel scientifique ou économique du pays et d'en informer sans délai les ministres compétents."

Renseignement ou information ?

Il convient ici de se référer à ce que, dans le monde du renseignement, on appelle traditionnellement "le cycle du renseignement" dans lequel on distingue "renseignement" et "information".

Un renseignement est une information traitée et analysée. Cette distinction est d'un intérêt pratique et sur le plan de la langue exprime plus précisément le concept du travail de ces services.

Les mots "renseignement" et "information" n'ont pas la même signification. Le dictionnaire "Le petit Larousse illustré" en donne la définition suivante :

a. Renseignement : *"Ensemble des connaissances de tous ordres sur un adversaire potentiel, utiles aux pouvoirs publics et au commandement militaire".*

b. Information : *“Elément de connaissance susceptible d’être codé pour être conservé, traité ou communiqué.”*

Le Comité R propose de définir le renseignement stratégique de la manière suivante :

“Action de coordonner la récolte, le traitement et l’analyse des informations dans le contexte politique, économique, social et militaire d’un ou de plusieurs pays.” ⁽¹⁾

Le Comité R propose dès lors de remplacer le mot “renseignement” par le mot “information”.

2. l’article 10 § 3 dernier alinéa évoque la question de la diffusion du renseignement :

“Ces renseignements ne peuvent être communiqués qu’aux ministres et aux autorités judiciaires et administratives concernées, aux services de renseignement et de sécurité, et aux services de police qui en ont besoin pour l’exécution de leurs missions.”

a. Le Comité R estime que la diffusion du renseignement est une mission essentielle des services de renseignement. Elle est reprise dans la définition du mot “renseignement”. Il convient dès lors d’insérer le concept de diffusion de renseignement dans les articles 7 et 9 de la loi.

Le Comité R a aussi relevé que la note d’orientation gouvernementale du 24 novembre 1995 prévoyait (p.79 du rapport annuel d’activités 1995 du Comité R) *“les services de renseignement transmettent d’initiative toute information qu’ils détiennent, susceptibles d’intéresser une autorité administrative ou judiciaire déterminée”*.

Le Comité R propose dès lors d’insérer à la fin du premier paragraphe 1° de l’article 7 du projet de loi, en vue de permettre aux communautés et aux régions de bénéficier du renseignement, une phrase à la fin de ce paragraphe qui pourrait être rédigée comme suit :

“et toute autorité administrative ou judiciaire concernée qui a intérêt à en connaître selon les modalités à délibérer par arrêté royal délibéré en conseil des ministres”.

Cette suggestion est le résultat notamment de l’enquête que le Comité R a menée à propos de l’efficacité et de la coordination des services de renseignement au sujet des activités des sectes. Cette recommandation est à mettre en parallèle avec l’article 10 § 3 alinéa 3 du texte du projet de loi qui traite de la problématique de la diffusion du renseignement.

b. Il apparaît de la lecture de l’exposé des motifs du projet de loi que le gouvernement ne fait pas la distinction entre la diffusion du renseignement et la collaboration des services de renseignement et de sécurité belge avec les services de renseignement étrangers.⁽¹⁾

En effet, il est indiqué dans l’exposé des motifs en ce qui concerne l’article 10 :

“Par ailleurs, les services de renseignement et de sécurité peuvent entretenir des relations directes et échanger des correspondances avec les autorités belges, étrangères ou

⁽¹⁾ Comité R - rapport d’activités - 1997 - Titre II “Enquête sur la création éventuelle d’un nouveau service de renseignement militaire”.

⁽²⁾ Doc., parl. Sess. Ord. 1995-1996 - 638 / 1 - 95 / 96 p. 14

internationales dont la collaboration est utile à l'exécution de leurs missions. Le paragraphe 3, alinéa 3, concerne aussi les échanges d'informations avec les services de renseignement et de sécurité belge et étrangers."

3. l'article 7 §1^{er} 2°

Le Comité R pense que pour respecter l'avis du Conseil d'Etat ⁽¹⁾ fondé sur la jurisprudence de la Cour européenne des droits de l'Homme (C.E.D.H.), il convient de supprimer les mots "conformément aux directives du Comité ministériel" et de les remplacer par "en vertu d'une loi."

Le Comité R a examiné l'arrêt Lüdi (C.E.D.H., 15 juin 1992 ⁽¹⁾) invoqué par le gouvernement dans l'exposé des motifs du projet de loi ⁽¹⁾ pour démontrer qu'il entendait respecter la jurisprudence de la C.E.D.H. Cet arrêt ne concerne pas les services de renseignement mais bien l'application des règles relatives au procès équitable concernant les activités d'un service de police. Il n'est donc pas d'application dans le cas d'espèce. Seuls les arrêts mentionnés par le Conseil d'Etat doivent être pris en considération (arrêts Malone et Leander).

Article 9 : missions du SGR

L'article 9 § 1^{er} 1° et 4°

Le Comité R estime devoir faire les mêmes remarques que pour les missions de la Sûreté de l'Etat.

En résumé :

- le 1° devrait reprendre le mot "information" à la place du mot "renseignement" et la phrase suivante devrait être ajoutée à la fin de ce paragraphe : "*et toute autorité judiciaires et administratives concernée qui a intérêt à en connaître selon les modalités à délibérer en conseil des ministres*".
- au 4°, les mots "conformément aux directives de Comité ministériel" devraient être remplacés par "en vertu d'une loi" en vue de respecter la jurisprudence de la C.E.D.H.

CHAPITRE III : L'exercice des missions

Article 10 : l'exercice des missions de renseignement et de sécurité ou les méthodes

1. Le Conseil d'Etat a, à juste titre, fait observer que le projet ne respectait pas la jurisprudence de la C.E.D.H. ⁽¹⁾

(1) Doc. parl précité p. 34 de l'avis du Conseil d'Etat et p. 9 de l'exposé des motifs du projet de loi, Doc. parl. précité

(2) La Revue trimestrielle des droits de l'homme , 1993, pp. 309-334

(3) Doc. parl. sess. ord. 1995-1996 - 638 / 1 - 95 / 96 p. 5

(4) Doc. parl précité pp. 31 et 35

Le Conseil d'Etat relève que le projet de loi ne respecte pas les arrêts Leander et Malone rendus par la C.E.D.H. Le Conseil d'Etat insiste en précisant que le projet de loi est dépourvu de règles claires et détaillées ayant trait à la collecte et l'usage d'informations et aux méthodes dont les services de renseignement et de sécurité peuvent faire usage.

En réponse le gouvernement fait état de l'arrêt Lüdi du 15 juin 1992. Le Comité R expose que cet arrêt ne concerne pas les services de renseignement mais bien les services de police. Il n'est donc pas d'application dans le cas d'espèce.

Le Comité R s'en réfère dès lors à l'avis du Conseil d'Etat.

2. l'article 10 § 1^{er} :

“Pour accomplir leurs missions, les services de renseignement et de sécurité ne peuvent utiliser des moyens de contrainte que dans les conditions prévues par la loi”.

Le Comité R estime que les méthodes utilisées généralement par les services de renseignement étrangers constituent des moyens de contrainte, à savoir :

- l'interception de correspondances écrites ;
- la pénétration et la fouille de lieu habité ;
- la filature et l'observation de personnes, de réunions, de rassemblements ;
- l'utilisation des moyens optiques de surveillance
- le recueil de données à caractère personnel.

Le Comité R rappelle dès lors qu'il faudra légiférer sur ces méthodes en vue de permettre l'exercice contrôlé des missions des services de renseignement.

Le Comité R n'ignore pas que les projets de loi sur les écoutes administratives et les enquêtes de sécurité sont en cours d'élaboration. Ils ne suffiront pas.

Le projet de loi ne mentionne pas le recours aux informateurs parmi les méthodes nécessitant une habilitation légale.

En ce qui concerne le recours à des informateurs spontanés et bénévoles, le Comité R est d'avis qu'il s'agit d'un moyen ne requérant pas d'autorisation particulière. Excepté la protection du secret, aucune autre disposition particulière ne semble devoir être prise en la matière.

Le Comité R pense que le recours à des informateurs rémunérés doit faire l'objet de certaines mesures. Il s'agit en effet d'une méthode de travail utilisant les deniers publics.

D'autre part, solliciter le concours de personnes extérieures au cadre des services de renseignement est une action susceptible de mettre la sécurité de ces personnes en danger. Il importe aussi de prévoir des règles de fiabilité et d'évaluation des informateurs.

Enfin, ce recours constitue aux yeux du Comité R un moyen de contrainte à l'égard de la personne sur qui des informations sont recueillies par des informateurs.

En ne prévoyant pas ces méthodes pour les services de renseignement, on peut craindre qu'ils ne se mettent en état de dépendance vis-à-vis des services de police et ou des services de renseignement étrangers.

Pour terminer sur le chapitre des méthodes, l'avis que le Comité R formule est basé sur l'étude comparative des législations allemande, italienne, britannique, canadienne, américaine et portugaise. Toutes ces législations, sans exception, stipulent la possibilité pour les services de renseignement d'utiliser les méthodes qui sont mentionnées ci-dessus et qui ne sont pas reprises dans le projet de loi.

Il est essentiel de prévoir un contrôle très strict de la bonne utilisation de ces méthodes.

3. l'article 10 § 3 alinéa 1 et 2

“Dans l'exercice des missions qui leur sont confiées, ils peuvent traiter ces données et ces informations et tenir à jour une documentation relative notamment à des événements, à des groupements et à des personnes présentant un intérêt pour l'exécution de leurs missions.

Les renseignements contenus dans la documentation doivent présenter un lien avec la finalité du fichier et se limiter aux exigences qui en découlent.”

Si ce texte de l'article 10 § 3 alinéa 1 et 2 est relatif à la protection de la vie privée et au secret, le Comité R estime alors que cet aspect devrait être repris au chapitre IV de la loi intitulé : “le secret”.

En outre, il convient de mentionner le terme information au troisième alinéa de ce paragraphe car ce sont les informations et non les renseignements qui sont contenues dans un fichier.

4. l'article 10 § 4

du projet de loi stipule :

“Les services de renseignement et de sécurité veillent à assurer une coopération efficace.”

Ce paragraphe est consacré à la collaboration entre les services de renseignement.

Le Comité R estime que cet aspect des activités des services concernés est tellement important qu'il devrait être repris dans un chapitre propre à cette matière.

La coopération relève davantage du domaine économique que de la sphère du renseignement⁽¹⁾.

Le terme “collaboration” convient mieux que le mot “coopération” et signifie globalement la même chose.

Il convient de rappeler à ce stade de l'étude du projet de loi que le gouvernement a créé un collège du renseignement et de la sécurité par arrêté royal du 21 juin 1996.

Ce collège est principalement chargé de la coordination opérationnelle des missions et n'est pas destiné à assurer la collaboration des activités des services de renseignement qui s'effectue avant

⁽¹⁾ “Le Petit Larousse Illustré”, 1995, p. 270

toute coordination.

Un protocole d'accord entre la Sûreté de l'Etat et le SGR a été ratifié. Comme indiqué lors de l'examen de l'article 2 du projet de loi, la gendarmerie et la Sûreté de l'Etat tentent de finaliser un accord visant à décrire les sujets sur lesquels ils collaboreront.

Le Comité R se réjouit de ces initiatives mais estime qu'il est essentiel que le projet de loi aille au-delà de l'obligation de respecter ce principe par la Sûreté de l'Etat et le SGR.

Le projet de loi devrait mentionner, dans un seul article, les modalités de la collaboration, entre :

1. les services de renseignement et de sécurité, eux mêmes;
2. les services de renseignement et de sécurité et les services de police;
3. les services de renseignement et de sécurité belges et les services de renseignement étrangers;
4. et, les autorités administratives, judiciaires et les services concernés, devraient être fixés par arrêté royal délibéré en conseil des ministres.

L'exposé des motifs du projet de loi mentionne la collaboration des services de renseignement et de sécurité belge avec les services de renseignement étrangers aux explications fournies en ce qui concerne l'article 10 § 3 dernier alinéa, comme indiqué ci-dessus.

Concernant la transmission des délits par les services de renseignement au parquet ou à la police, le Comité R souhaite se référer à la législation allemande, extrêmement claire sur le sujet. Le Comité R renvoie le lecteur à son rapport annuel d'activités 1996 page 17 :

“En Allemagne, la séparation entre services de renseignement et service de police est respectée : les agents des services de renseignement n'ont aucune compétence d'officier de police judiciaire. Il en résulte qu'il n'y a pratiquement pas de conflit de compétence entre services de police et services de renseignement. Dès lors que ces derniers détiennent des indices d'infractions pénales, ils les transmettent au parquet ou aux services de police.

Néanmoins, le législateur allemand permet aux services de renseignement d'apprécier la nécessité d'une telle communication en fonction de la gravité du délit d'une part, et de l'importance des opérations qu'ils mènent d'autre part. Les services de renseignement peuvent s'accorder avec le procureur général à cet égard. Le § 138 de la “Strafprozessordnung” définit cependant quels sont les crimes qui doivent être obligatoirement portés à la connaissance de la Justice. Le Comité R recommande que l'article 29 du Code d'instruction criminelle soit amendé en ce sens”.⁽¹⁾

Articles 11 à 22 : mission de protection rapprochée assurée uniquement par la Sûreté de l'Etat

⁽¹⁾ “Toute autorité constituée, tout fonctionnaire ou officier public qui, dans l'exercice de ses fonctions, acquerra la connaissance d'un crime ou d'un délit, sera tenu d'en donner avis sur-le-champ au Procureur du Roi près le tribunal dans le ressort duquel ce crime ou ce délit aura été commis ou dans lequel l'inculpé pourrait être trouvé, et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs(...)”.

Les agents de la Sûreté de l'Etat ne bénéficient pas de la qualité d'officier de police judiciaire. La qualité d'officier de police administrative est non écrite mais décrite dans le projet de loi. Les agents de la Sûreté de l'Etat doivent bénéficier de cette dernière qualité pour effectuer leur mission de protection rapprochée.

Le Comité R estime que c'est une bonne solution qui permet une exécution souple de cette mission.

Le Comité R attire, ici, l'attention du législateur sur l'article 11 de la loi sur la fonction de police qui prévoit : *“ Le Roi détermine les cas dans lesquels le ministre de l'Intérieur fait assurer la protection spéciale des personnes et des biens mobiliers et immobiliers. Il fixe les modalités de cette protection”*.

Le Comité R rappelle qu'aucun arrêté royal n'a jusqu'à présent été publié au Moniteur belge.

CHAPITRE IV : Le secret

Le Comité R constate que la notion de secret est définie aux articles 23, 24, et 25.

Le Comité R, estime toutefois qu'il convient aussi d'aborder dans la loi, le secret de l'information elle-même, c'est-à-dire le contenu de l'information. Ce dernier aspect du secret peut être réglé par des modalités de classification du document comme l'écrit le Conseil d'Etat (pp. 34 et 35 du document parlementaire précité) :

“Il convient ... qu'il établisse au moins les principes essentiels de la classification, parmi lesquels, notamment, les relations convenables entre les divers degrés de la classification ainsi que la nature et l'étendue des investigations auxquelles l'enquête précédant l'habilitation à accéder aux lieux, documents et autre matériel ainsi classifiés pourrait donner lieu.”

Enfin, un conflit pourrait se présenter entre, d'une part, les intérêts de la Sûreté de l'Etat ou du SGR, d'après lesquels le secret de certaines sources et données pourrait être nécessaire et, d'autre part, l'intérêt de la recherche de la vérité dans une procédure judiciaire.

Laisser la notion du secret d'Etat à la seule appréciation d'un agent des services de renseignement ne paraît pas opportun.

Le Comité R propose que cet aspect du problème soit, d'une part, inscrit dans la loi et, d'autre part, soit de la compétence de deux ministres (dont le ministre responsable) ou du conseil ministériel.

Ce système (deux ministres - dont le ministre responsable) est d'application aux Pays-Bas et garantit l'obligation pour les membres des services de renseignement de ne pas se soustraire unilatéralement à leur devoir testimonial, ce qui fut le cas lors de l'enquête parlementaire sur l'existence en Belgique d'un réseau de renseignement clandestin international.

CHAPITRE V : Dispositions modificatives et finales

Article 26

“L'article 259bis du Code pénal est complété par un § 5 rédigé comme suit :

§ 5. Les dispositions du § 1^{er}, 1° et 2°, ne s'appliquent pas à la captation, l'écoute, la prise de

connaissance ou l'enregistrement, par le service général du renseignement et de la sécurité des Forces armées, à des fins militaires, de radiocommunications militaires émises à l'étranger."

Il est urgent qu'une disposition légale autorise cette méthode.

Le Comité R signale que cet article ne règle que partiellement la problématique des interceptions militaires.

1. Le Comité R recommande avec insistance que la loi vise également la captation de signaux radio émis par voie d'ondes électromagnétiques telles que les signaux radars, par exemple.
2. Le Comité R estime également qu'il faudrait mentionner que cet article 26 déroge non seulement aux articles 259 bis et 314 bis du Code pénal mais aussi à l'article 111 de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques et économiques et l'article 4c de la loi du 30 juillet 1979 et l'arrêté loi du 16 octobre 1916. Ces articles de loi prohibent les interceptions de télécommunication. La radio communication est comprise dans la télécommunication.
- 3 D'autres unités que le SGR procèdent à des interceptions ce qui sur le plan de la technique juridique est en violation avec la loi de 1979 et celle de 1991 mentionnées ci-dessus. Le Comité R vise ici les interceptions par radar pratiquées par les F16, les C130 etc.

CHAPITRE 2 : LES DROITS D'ACCÈS DU PARTICULIER À SON DOSSIER INDIVIDUEL AUPRÈS D'UN SERVICE DE RENSEIGNEMENT

1. INTRODUCTION

Dans une interview publiée par le journal "Het Volk" le 21 janvier 1995, l'Administrateur général de la Sûreté de l'Etat explique qu'en principe, chaque citoyen qui a des raisons de croire que la Sûreté a établi un dossier à son nom a le droit d'en prendre connaissance, sauf si la Sûreté estime que cela menace l'ordre public et l'intérêt de la Défense nationale. Dans la foulée de son enquête sur la destruction des dossiers des services de renseignement, le Comité R a décidé de s'intéresser au problème de l'accès des particuliers aux dossiers que ces services ont établis sur eux.

La décision de mener cette étude a été prise par le Comité R en date du 5 mars 1996.

2. MOTIF DE L'ÉTUDE

La présente étude s'inscrit dans la mission fondamentale du Comité R qui est de garantir la protection des droits que la Constitution et la loi confèrent aux personnes (article 1^{er} de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements); elle trouve son fondement légal dans cette disposition.

Le Comité R a estimé qu'il était important d'effectuer cette étude afin de faire la synthèse des droits dont le citoyen dispose pour accéder à son dossier individuel auprès des services de renseignement.

3. L'INTÉRÊT DES PARLEMENTAIRES POUR LE PROBLÈME

Le Comité R a dénombré quatre questions parlementaires sur le sujet.

3.1. Chambre des Représentants

3.1.1. Question au ministre de l'Intérieur

Le 26 octobre 1995, question orale du député Deleuze (ECOLO) intitulée "*Surveillance d'associations et de partis politiques par des écoutes téléphoniques*" (Chambre des représentants - compte rendu analytique - 26/10/95 - p. 282) : malgré son titre, cette question ne concerne pas l'interception de communications mais bien la base légale de la surveillance des

mouvements pacifistes et écologistes :

“Le 12 octobre dernier, le ministre de la Défense nationale a reconnu que les mouvements pacifistes et écologistes étaient soumis à une surveillance par l'appareil d'Etat. Quelle est la base légale de cette surveillance ? Les parlementaires, membres de ces mouvements, sont-ils surveillés ? Où s'arrête la surveillance en fonction de l'activité concernée ? Aurons-nous la possibilité de prendre connaissance des fiches qui nous concernent ?”

Réponse

En ce qui concerne les fiches, il y a une loi qui prévoit que chaque individu peut vérifier si les données le concernant sont correctes. Il doit le faire via une commission chargée spécifiquement de vérifier la véracité des données.

3.1.2. Question au ministre de la Justice

Question n° 834 de M. Decroly (ECOLO) du 7 février 1995 : Sûreté de l'Etat - dossiers individuels - consultation.

Faisant référence à l'interview de Monsieur Van Lijsebeth publiée au journal “Het Volk” le 21 janvier 1995, le député demande notamment :

- “1. Quelle est la procédure à suivre et quelles sont les coordonnées du (des) service(s) compétent(s) pour recevoir de telles demandes de consultation ?*
- 2. Au cours des trois dernières années, combien de citoyens ont accompli cette démarche et combien ont vu leur demande satisfaite ?*
- 3. Quel(s) critère(s) définit (définissent) la “raison d'Etat” qui, selon cet article, peut être invoquée pour refuser à un citoyen l'accès à son dossier ?”*

Réponse

Le ministre dans sa réponse s'en réfère à la loi du 11 avril 1994 relative à la publicité de l'administration.

Il précise : *“Depuis le 1er juillet 1994, date d'entrée en vigueur de la loi du 11 avril 1994, quatre demandes de consultation ont été introduites auprès de l'Administration de la Sûreté de l'Etat. L'une était adressée erronément à la Sûreté de l'Etat. La deuxième a été rejetée et les deux autres sont à l'examen.*

L'article 6, § 1^{er} à 3, de la loi, énumère une série de cas dans lesquels l'obligation de publicité ne s'applique pas. Les motifs énoncés à l'article 6, § 1^{er} et 2 protègent des intérêts fondamentaux et ont un caractère obligatoire pour l'autorité administrative si, après avoir mis en balance l'intérêt d'un ou plusieurs motifs d'exception et l'intérêt de la publicité, elle constate que la publicité ne l'emporte pas sur la protection de l'intérêt en cause.”

3.2. Sénat

3.2.1. Question au ministre de l'Intérieur

Le 8 décembre 1995, question n° 63 de M. Boutmans (AGALEV) intitulée “*Accord de Schengen - Correction des données fournies par le demandeur d’asile*”
(Questions et réponses - Sénat - 16 janvier 1996 (n° 1-8).

3.2.2. Question au ministre de la Justice

Question n° 975 de M. Buelens (VBL) du 14 février 1995 : demande de consultation de dossiers personnels.

Faisant référence à l’interview de Monsieur Van Lijsebeth publiée au journal “Het Volk” le 21 janvier 1995, le sénateur demande notamment :

1. *Quelles démarches un particulier doit-il concrètement entreprendre :*
 - a) *pour savoir s’il y a un dossier à son nom;*
 - b) *pour pouvoir consulter ce dossier ?*
2. *Quelles directives l’administration concernée a-t-elle reçues pour répondre à pareilles demandes de consultation de dossier personnel ? Où et comment un demandeur peut-il aller en appel contre un refus éventuel de pareille consultation ?”*

Réponse

Le ministre s’en réfère à la loi du 11 avril 1994 relative à la publicité de l’administration.

4. SITUATION À L’ÉTRANGER

FRANCE

Le Comité R a pris connaissance du 13ème rapport annuel (1992) de la Commission Nationale Informatique et Libertés (CNIL).

L’article 39 de la loi du 6 janvier 1978 prévoit l’accès indirect pour les “traitements intéressant la Sûreté de l’Etat, la défense et la sécurité publique”. L’accès direct est totalement interdit.

Un décret a été pris le 14 octobre 1991 et appliqué en 1992. Il apporte une transparence accrue des fichiers en fixant de nouvelles modalités d’exercice du droit d’accès.

Le rapport annuel de la CNIL précise les conditions de cet accès : “*La CNIL, en accord avec le ministre de l’Intérieur, peut constater que la communication de certaines informations ne met pas en cause la Sûreté de l’Etat, la défense et la sécurité publique et qu’il y a donc lieu de les transmettre à l’intéressé selon l’une des procédures suivantes :*

- *la CNIL indique au requérant, en accord avec le ministre de l’Intérieur, que les renseignements généraux ne détiennent aucune information le concernant;*
- *la CNIL communique au requérant, en accord avec le ministre de l’Intérieur, tout ou partie des informations le concernant détenues par les renseignements généraux;*
- *le ministre de l’Intérieur peut en effet s’opposer à la communication, totale ou partielle, au requérant des informations le concernant lorsque cette communication peut nuire à la Sûreté de l’Etat, à la défense ou à la sécurité publique; dans ce cas la Commission informe le requérant*

qu'il a été procédé aux vérifications. Cette décision de refus de communication peut être contestée devant le Conseil d'Etat."

Le rapport de 1992 indique en outre que :

"Depuis l'entrée en vigueur du décret du 14 octobre 1991 (avril 1992), le traitement des demandes d'accès aux fichiers des renseignements généraux a conduit aux résultats suivants :

- *56% des requérants n'étaient pas fichés ;*
- *lorsqu'un dossier existait :*
 - * *il a été considéré dans 25% des cas comme non communicable par les membres de la CNIL chargés du droit d'accès indirect;*
 - * *sa communication a été acceptée en totalité dans 58 % des cas, et partiellement dans 14% des cas ;*
 - * *sa communication, demandée par la CNIL, a été refusée par le ministère de l'Intérieur dans 3 % des cas."*

CANADA

Le Comité R a pris connaissance d'un article paru dans "Le Monde du Renseignement" le 22 octobre 1992 qui indique :

"Le SCRS (service canadien du renseignement de sécurité) veut échapper à la loi sur les libertés. Le SCRS a proposé de créer une banque de données devant explicitement échapper aux dispositions de la loi sur les libertés individuelles. Si le SCRS peut refuser aux particuliers l'accès aux informations secrètes, il souhaite cependant "simplifier la situation" en faisant établir que pour des motifs de sécurité nationale, certaines informations ne sont pas accessibles au public".

Désirant vérifier cette information, le Comité R a écrit à son homologue canadien, le Comité de surveillance des activités de renseignement de sécurité (CSARS) qui très aimablement lui a adressé la réponse suivante le 28 janvier 1997 :

"...la problématique que vous soulevez relève davantage de la compétence du Commissaire à la protection de la vie privée que celle du Comité de surveillance."

La "nouvelle parue dans le journal "Le Monde du Renseignement" du 22 octobre 1992 fait état des démarches prises par le SCRS (service canadien du renseignement de sécurité) pour créer un fichier inconsultable. Vous trouverez, en annexe, une description des informations contenues dans le fichier SRS SDS 010. En général, ce fichier contient des renseignements sur les personnes qui font l'objet d'une surveillance par le SCRS, laquelle est dûment approuvée, ou qui sont entrées en contact avec des personnes ou des groupes surveillés. Avant les démarches du SCRS, ces fichiers étaient officiellement ouverts mais dans les faits, le SCRS répondait toujours aux demandes de renseignements contenus dans ce fichier sans confirmer ou nier l'existence de renseignements personnels, ce qui risquait d'induire le public en erreur. Il a donc été jugé préférable que le SCRS crée officiellement un fichier inconsultable dûment constitué.

Cette approche signifie simplement qu'il serait préjudiciable aux activités du SCRS que quelqu'un sache qu'il ou qu'elle est surveillé(e) ou non par le SCRS. Le Commissaire à la vie privée et la Cour fédérale ont tous deux appuyé ce principe dans l'affaire Jamshid Zanganeh c./ le service canadien du renseignement de sécurité. Soit dit en passant, c'est aussi par respect pour ce principe que le

Comité évite de confirmer ou de nier à la personne qui se plaindrait des agissements du SCRS à son égard qu'elle est ou non une cible du SCRS. Dans tous les cas, nous nous assurons toutefois que le Service n'a pas exercé et n'exerce pas ses pouvoirs de façon abusive ou inutile; et que l'exercice des fonctions du SCRS est à la fois efficient, efficace et conforme à la loi.

Enfin, la création d'un fichier inconsultable impose une lourde responsabilité supplémentaire au commissaire, qui doit s'assurer que le fichier inconsultable ne contiendra que des renseignements à caractère extrêmement délicat. Le Commissaire a déjà énoncé une mise en garde à l'effet qu'après avoir autorisé la création d'un tel fichier, on lui permette de devenir sans contrôle, un dépôt secret de renseignements personnels. L'article 36 de la loi sur la protection des renseignements personnels reconnaît d'ailleurs le rôle du Commissaire en lui donnant le pouvoir de tenir des enquêtes sur ces fichiers et de recommander que les dossiers qu'ils contiennent soient versés dans des fichiers ouverts, de demander à la Cour fédérale d'ordonner le retrait des dossiers en question si le SCRS n'accepte pas sa recommandation et, bien entendu, de signaler tout refus du SCRS d'appliquer ses recommandations.

Le bureau du Commissaire a toujours été très clair quant à son interprétation de la disposition autorisant la création de fichier inconsultable : refuser l'accès à un fichier inconsultable n'est pas une obligation mais plutôt une décision discrétionnaire.

Je terminerai en citant la position donnée par le Commissaire :

"La façon honnête de procéder consiste à rendre le fichier inconsultable pour dissiper la confusion sur l'accessibilité des renseignements, tout en mettant en place des mécanismes appropriés pour que ce fichier inconsultable soit utilisé avec discernement".

La personne responsable termine sa lettre en donnant les coordonnées du Commissaire à la protection de la vie privée du Canada.

SUISSE

Le Comité R a pris connaissance d'un article paru dans "Le Monde du Renseignement" le 27 août 1992 :

"L'Ombudsman du renseignement s'active. René Bacher, le nouveau médiateur pour les dossiers de renseignements personnels, a adressé une lettre aux 39.000 personnes qui ont demandé accès à leur dossier pour les prier de patienter. La procédure ne pourra commencer qu'une fois que les deux chambres se seront définitivement entendues sur les termes de la loi. Le Conseil national prône une mouture restrictive en raison des ... implications financières. S'il n'y a pas d'accord, Monsieur Bacher sera contraint de licencier une partie de ses 39 salariés. (...)"

Le Comité R a estimé intéressant de demander aux autorités helvétiques la manière dont cette problématique était réglée dans leur pays.

Il ressort des renseignements obtenus auprès du "préposé spécial au traitement des documents établis pour assurer la sécurité de l'Etat" que :

- 1) Cette matière est réglée en Suisse par l'arrêté fédéral du 9 octobre 1992 et l'ordonnance du 20 janvier 1993 sur "la consultation des documents du Ministère public de la Confédération".
- 2) L'arrêté fédéral s'applique à tous les documents du service de police du Ministère public de la

Confédération qui lui ont été remis avant le 16 mai 1990.

- 3) Le droit des citoyens de consulter les documents est accordé lorsque la personne concernée fait état d'un préjudice matériel ou moral vraisemblable en rapport avec des informations contenues dans des documents du service de police.
- 4) L'arrêté fédéral prévoit que le droit de consulter des documents est refusé, limité ou différé lorsque des intérêts publics ou privés prépondérants, une procédure judiciaire en cours ou des obligations de maintien du secret, l'exigent.
- 5) Le Conseil fédéral définit les cas de dérogation à l'autorisation de consultation du dossier.
- 6) Un "*préposé spécial*" nommé par le Conseil fédéral est chargé de statuer sur les demandes de consultation. Il s'efforce de parvenir tout d'abord à un accord avec le demandeur.
- 7) Les personnes qui n'ont présenté aucune demande de consultation avant le 1^{er} avril 1990 ont dû déposer leur requête de consultation dans les 6 mois qui ont suivi l'entrée en vigueur de l'arrêté fédéral du 9 octobre 1992.
- 8) Lorsque la demande de consultation est complète ou qu'elle a été complétée dans le délai imparti, le "*préposé spécial*" examine la vraisemblance du dommage invoqué.
- 9) Lorsque les conditions de la consultation de documents sont réunies, le "*préposé spécial*" envoie au requérant une copie des documents relatifs à la demande.
- 10) L'article 9 de l'ordonnance du 20 janvier 1993 prévoit :

Lorsqu'un intérêt public prépondérant l'exige, la consultation est refusée, limitée ou différée. Un tel intérêt existe lorsque la poursuite de l'activité de protection de l'Etat ou la sûreté intérieure ou extérieure du pays risquerait d'être sérieusement compromise par :

- a) la divulgation d'importants renseignements sur le terrorisme, sur l'extrémisme violent, sur l'espionnage ou sur le crime organisé, ou par
- b) la révélation d'importants dispositifs, d'ordre tactique ou opérationnel, des autorités chargées de la protection de l'Etat.

Le nom des collaborateurs chargés des dossiers est caviardé.

Les indications relatives à des tiers sont caviardées lorsque ces tiers ont un intérêt privé primordial à ce qu'elles le soient. Un intérêt privé est notamment primordial si :

1. des informations relatives à la sphère privée protégée de tiers, ou
2. des informations sur des personnes ayant fourni en toute bonne foi des renseignements à la police seraient divulgués

La consultation est en outre refusée, limitée ou différée lorsque les informations divulguées risqueraient :

- a) de compromettre une procédure en cours ou
- b) de violer l'obligation de maintien du secret vis-à-vis de services étrangers de renseignements ou de sécurité.

- 11) En ce qui concerne la rectification de certaines données figurant dans le dossier, l'ordonnance prévoit que lorsqu'une personne conteste l'exactitude de certaines données, elle peut exiger qu'une mention appropriée figure sur les documents ou leur soit annexée.

Lorsque des documents sont manifestement erronés, ils sont rectifiés à la demande de la personne concernée.

La procédure pénale de droit commun s'applique à la procédure prévue dans l'ordonnance du 20 janvier 1993.

En ce qui concerne le nombre de demandes de consultation enregistrées, il a été précisé par le "préposé spécial" que sur une période de six années, environ 300.000 personnes ont demandé si elles étaient répertoriées.

Environ 40.000 d'entr'elles l'étaient et celles-ci ont reçu copie de leur fiche expurgée des mentions sensibles.

Environ 7.000 personnes ont insisté pour avoir accès à leur dossier. Environ 1 million de pages (pour la plupart des rapports de police) ont été remises aux intéressés.

PAYS-BAS

Avant le 16 juin 1994, un particulier n'avait pas en principe accès à son dossier détenu par le BVD (Binnenlandse Veiligheidsdienst).

Le Conseil d'Etat a renversé cette jurisprudence dans les arrêts Van Baggum et Valkenier.

Le Conseil d'Etat donne les explications suivantes dans un communiqué de presse :

Concerne : Van Baggum et Valkenier

"Aujourd'hui (le 16 juin 1994) la section administrative du Conseil d'Etat a rendu un arrêt dans deux affaires dans lesquelles deux citoyens avaient demandé si le BVD avait constitué des dossiers les concernant. Dans l'affirmative, ils demandaient à avoir accès à leurs dossiers.

La section administrative du Conseil d'Etat a jugé que l'article 16 de la loi sur les services de renseignements et de sécurité, qui règle entre autres la publicité des dossiers du BVD, n'est pas d'application car cet article est contraire aux articles 8 et 13 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales. Cette jurisprudence se base notamment sur des arrêts rendus par la Cour Européenne des droits de l'homme à Strasbourg.

Cette section a ensuite examiné les requêtes des citoyens sur base de la loi sur la "publicité de l'administration" (Wet openbaarheid van Bestuur). Le point de vue du ministre de l'Intérieur n'a pas été suivi par la section. Selon le ministre, le seul fait que le BVD soit en cause, signifie que la sûreté de l'état ne permet pas de répondre à la requête des citoyens.

La section a donc annulé la décision du Ministre dans ces deux affaires. Le Ministre devra à nouveau décider en tenant compte des arrêts rendus."⁽¹⁾

Le rapport annuel 1995 du BVD mentionne :

⁽¹⁾ Traduction libre

“La conséquence directe de cette jurisprudence implique que les demandes d'accès encore en cours devront être appréciées, cas par cas, sur base des critères prévus par la loi relative à la “publicité de l'administration”.

Cela constitue un exercice de travail administratif intense. La réponse à une requête d'accès ne peut permettre la prise de connaissance du travail actuel, des sources et de la méthode de travail du BVD car cela pourrait nuire au fonctionnement de ce service ainsi qu'à la sûreté de l'état pour laquelle il travaille.⁽¹⁾

Le BVD réexamine un nombre important de dossiers compte tenu de cette jurisprudence. Fin 1996, les retards pourront être résorbés dans des proportions acceptables grâce à l'engagement de personnel supplémentaire.

La loi sur les services de renseignements et de sécurité reste d'application en ce qui concerne les demandes d'accès de tiers aux données détenues par le BVD. Cela implique que des données personnelles ne peuvent être communiquées à un tiers qu'en cas de nécessité pour l'exécution de la mission légale du BVD.

La jurisprudence de la section administrative du Conseil d'Etat citée ci-dessus dans les affaires Van Baggum et Valkenier a directement donné lieu à une procédure de modification de la loi du 3 décembre 1987 sur les services de renseignements et de sécurité.

Cette modification de loi est en cours.

5. LES PROCÉDURES D'ACCÈS DANS LA LÉGISLATION BELGE ACTUELLE

Dans l'Etat actuel de la législation, le Comité R a relevé deux procédures distinctes pouvant avoir comme effet d'ouvrir aux particuliers un accès direct ou indirect à leur dossier auprès des services de renseignement :

- une possibilité d'accès résulte de l'article 13, 2° de la loi du 8 décembre 1992 sur la protection de la vie privée;
- une deuxième possibilité résulte des articles 4 et 5 de la loi du 11 avril 1994 relative à la publicité de l'administration.

L'accès direct permet à un particulier de prendre connaissance en personne de son dossier détenu par un service de renseignement.

Il faut aussi noter que l'article 38.7 de l'accord de Schengen accorde, au demandeur d'asile qui en fait la demande, le droit de prendre connaissance des données communiquées qui le concernent, pour autant qu'elles soient disponibles, et de les corriger.

On entend par accès indirect le mandat que confie un particulier à un organisme qui a la possibilité de consulter le dossier de ce particulier constitué par un service de renseignement.

5.1. Accès indirect via la Commission de la protection de la vie privée

⁽¹⁾ Traduction libre

Une possibilité d'accès résulte de l'article 13, 2° de la loi du 8 décembre 1992 sur la protection de la vie privée.

Cet article dispose que : *“toute personne justifiant de son identité a le droit de s'adresser sans frais à la Commission de la protection de la vie privée pour exercer son droit et de rectification à l'égard :*

- 1° (...)
- 2° *des traitements gérés par l'administration de la Sûreté de l'Etat du ministère de la Justice ou par le Service général du Renseignement et de la Sécurité du ministère de la Défense nationale.”*

Ce recours ne donne toutefois qu'un droit d'accès indirect puisque l'alinéa 3 de l'article 13 précité énonce que : *“La Commission de protection de la vie privée communique uniquement à l'intéressé qu'il a été procédé aux vérifications nécessaires”.*

De plus, l'alinéa 2 de cet article 13 dispose que : *“Le Roi détermine, après avis de la Commission de la protection de la vie privée et par arrêté délibéré en Conseil des Ministres, les modalités d'exercice de ces droits”.*

L'arrêté royal est en cours d'élaboration (août 1997).

5.2. Accès par application de la loi du 11 avril 1994 relative à la publicité de l'administration

Une deuxième possibilité résulte des articles 4 et 5 de la loi du 11 avril 1994 relative à la publicité de l'administration. C'est à cette possibilité que l'Administrateur général de la Sûreté de l'Etat faisait allusion dans l'interview qu'il a accordée au journal "Het Volk".

Ces articles instituent et organisent le droit des particuliers de consulter sur place et de recevoir une copie d'un document administratif d'une autorité administrative fédérale.

L'article 6 prévoit une série de motifs pour rejeter une demande de consultation; il en est notamment ainsi lorsque l'intérêt de la publicité ne l'emporte pas sur la protection de l'un des intérêts suivants :

- 1° la sécurité de la population;
- 2° les libertés et les droits fondamentaux des administrés;
- 3° les relations internationales fédérales de la Belgique;
- 4 l'ordre public, la sûreté ou la défense nationales;
- 5° la recherche ou la poursuite de faits punissables;
- 6° un intérêt économique ou financier fédéral, la monnaie ou le crédit public;
- 7° le caractère par nature confidentiel des informations d'entreprises ou de fabrication communiquées à l'autorité;
- 8° le secret de l'identité de la personne qui a communiqué le document ou l'information à l'autorité

administrative à titre confidentiel pour dénoncer un fait punissable ou supposé tel.

L'article 6 § 2 stipule qu'une demande de consultation peut également être rejetée si la publication du document administratif porte atteinte à la vie privée d'une personne, à une obligation de secret instaurée par la loi ou au secret des délibérations du gouvernement et des autorités fédérales.

La Commission d'accès aux documents administratifs peut rendre un avis à l'occasion d'une "demande de reconsidération" d'un refus de communication. Cet avis ne lie pas l'autorité administrative fédérale. Un second refus ou l'absence de décision sur une demande de reconsidération peut faire l'objet d'un recours au Conseil d'Etat (art. 8, § 2, 4ème alinéa).

5.3. Accès par l'application de l'accord de Schengen

Le Comité R s'est demandé si l'article 38.7 de la Convention d'application de l'Accord de Schengen du 14 juin 1985 (Moniteur belge du 15 octobre 1993) n'offrait pas une voie d'accès aux dossiers individuels des services de renseignement. Cet article est ainsi libellé : *“Un demandeur d'asile a le droit de se faire communiquer, sur demande, les informations échangées le concernant, aussi longtemps qu'elles sont disponibles. S'il constate que ces informations sont inexactes ou n'auraient pas dû être transmises, il a le droit d'en exiger la rectification ou la disparition.”*

Les données qui peuvent être échangées à propos d'un demandeur d'asile sont définies à l'article 38. 2 de la Convention. Il s'agit essentiellement d'éléments nécessaires pour établir l'identité du demandeur ainsi que de données sur la demande d'asile elle-même. Parmi ces informations, figurent sous d) *“les lieux de séjour et les itinéraires de voyages”* du demandeur d'asile.

Or, l'article 99.3 de la Convention permet, *“aux fins de surveillance discrète”*, le signalement d'individus ou de véhicules dans Système d'Information Schengen (S.I.S.) par les *“instances compétentes pour la Sûreté de l'Etat”* (en Belgique, l'Administration de la Sûreté de l'Etat). Dans le cadre de cette surveillance discrète, certaines informations peuvent en tout ou en partie, être recueillies et transmises à l'autorité signalante, *“à l'occasion de contrôles de frontière ou d'autres contrôles de police et des douanes exercés à l'intérieur du pays”*. Parmi ces informations susceptibles d'être échangées, on retrouve sous c) *“l'itinéraire et la destination du voyage”*. Ce type de signalement peut être effectué *“lorsque des indices concrets permettent de supposer que les informations visées au paragraphe 4 sont nécessaires à la prévention d'une menace grave émanant de l'intéressé ou d'autres menaces graves pour la sûreté intérieure et extérieure de l'Etat.”*

Les seules données qu'un demandeur d'asile pourrait découvrir comme étant connues par la Sûreté de l'Etat sont les itinéraires et les destinations de ses précédents voyages. Ce signalement n'est pratiquement pas utilisé.⁽²⁾

6. L'APPLICATION DE CES LÉGISLATIONS

L'application de ces législations a été discutée lors d'une réunion tenue le 12 février 1996 au siège du Comité R et à laquelle assistaient des membres de la commission de la protection de la vie privée, d'une part, de la commission d'accès aux documents administratifs, d'autre part.

⁽²⁾ Rapport d'activités annuel du Comité R 1996 et 1997

6.1. L'application de ces législations par la Sûreté de l'Etat

Nombre de demandes introduites : durant la période 1995-1996, 109 demandes d'accès de particuliers à leur dossier individuel ont été introduites

Nombre d'acceptations : aucune.

Nombre de refus : les 109 demandes ont été refusées. Cependant un certain nombre de ces demandeurs ont reçu comme réponse qu'il n'y avait pas de dossier les concernant auprès de la Sûreté de l'Etat.

Dans les cas de refus portés à la connaissance du Comité R, le ministre de la Justice ou l'administrateur général de la Sûreté de l'Etat ont rejeté la demande d'accès introduite par un particulier en se basant sur l'article 6, § 1^{er}, 4^o (exception relative à la Sûreté nationale) et § 2, 1^o et 2^o (exception relative à la vie privée) de la loi du 11 avril 1994 précitée. Les motifs suivants ont été évoqués :

6.1.1. Exception relative à la sûreté nationale (article 6, §1er, 4°).

Le ministre de la Justice ou l'administrateur général de la Sûreté de l'Etat répond généralement que :

“La nature particulière des tâches de la Sûreté de l'Etat, service de renseignement et de sécurité, et le caractère secret de ses activités ont été reconnus par la Chambre et le Sénat lors des discussions parlementaires relatives à la loi organique du contrôle des services de police et de renseignements ainsi qu'à la loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel”.

La Sûreté de l'Etat relève qu'il a été déclaré à cet égard que :

“Les membres des services de renseignement sont habilités à recueillir et à traiter des informations sur des personnes en gardant ces activités secrètes”.

(Doc. Sénat 1258-2 (1990-1991) relatif au projet de loi organique du contrôle des services de police et de renseignements).

“La nature même des tâches qu'ils (la Sûreté de l'Etat du ministère de la Justice et le Service général du Renseignement et de la Sécurité du Ministère de la Défense nationale) accomplissent justifie qu'ils puissent continuer à l'accomplir avec toute la discrétion nécessaire”.

(Doc. Chambre n°1610/1 (90/91) p.8 concernant le projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel).

“La société a intérêt à voir respecter le secret du travail de ses services de renseignement”.

(Doc. Sénat 445-2 (91/92) p. 79 concernant le projet de loi relatif à la protection de la vie privée à l'égard des traitement de données à caractère personnel).

Or, dit M. Van Lijsebeth, *“la consultation des dossiers de la Sûreté de l'Etat permettrait de le deviner et ainsi de paralyser l'action de ce service en portant atteinte au caractère fondamentalement secret de ses activités”.*

6.1.2. Exception relative à la vie privée (article 6, § 2, 1° et 2°)

Selon la Sûreté de l'Etat, ses dossiers "contiennent essentiellement des données à caractère personnel "dites sensibles", au sens des art. 6, 7 et 8 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, tant en ce qui concerne le titulaire du dossier que le cas échéant, des tierces personnes".

En ce qui concerne la protection des données relatives à la vie privée de tierces personnes, l'exposé des motifs de la loi sur la publicité souligne en effet que "si l'autorité divulgue par exemple un document sans avoir veillé au droit d'un tiers au respect de sa vie privée ou sans avoir organisé d'une manière adéquate la mise en balance, elle manque à son devoir de minutie, ce qui met en cause sa responsabilité". (Doc. Chambre 1112/1 (92/93) p. 16).

Et la Sûreté de conclure : "Vu le caractère généralement sensible des renseignements recueillis par la Sûreté de l'Etat, il est essentiel que le respect de la vie privée de ces personnes soit absolu".

Quant à la consultation des données à caractère personnel concernant le titulaire du dossier, la Sûreté renvoie les demandeurs à l'article 13 de la loi du 8 décembre 1992 précitée, qui, par l'intermédiaire de la Commission de la protection de la vie privée, leur confère un droit "d'accès indirect" aux traitements automatisés et manuels de données à caractère personnel gérés par la Sûreté de l'Etat.

La Sûreté ajoute : "La compétence de cette Commission à l'égard de ces traitements de données est exclusive conformément à l'article 3 § 3 alinéa 2 de la loi du 8 décembre 1992 qui stipule que ladite Commission "est seule compétente pour assurer l'exercice du droit d'accès et de rectification de la personne concernée conformément à l'article 13".⁽³⁾

Selon la Sûreté, la loi du 8 décembre 1992 constitue une législation spécifique; elle comporte des dispositions plus strictes en matière de publicité et instaure en outre une obligation de secret. La loi de 1992 déroge donc au principe général de la publicité résultant de la loi du 11 avril 1994 et elle prévaut sur celui-ci.

Selon la Sûreté, "les exceptions à la publicité des documents administratifs énumérés à l'article 6 § 1 et 2 de la loi du 11 avril 1994 ont un caractère obligatoire à l'égard des autorités administratives fédérales ou non fédérales. En conséquence, celles-ci doivent rejeter la demande si, après avoir mis en balance l'intérêt de la publicité avec l'intérêt protégé par un ou plusieurs motifs d'exception, elles ont constaté que la publicité ne l'emporte pas sur la protection de l'intérêt en cause. Il est cependant à noter que lorsqu'une loi spécifique instaure une obligation de secret, il n'y a pas lieu de procéder à la mise en balance des intérêts. Dans ce cas le motif d'exception est absolu."⁽⁴⁾

A l'occasion d'un entretien avec un conseiller - adjoint à la Sûreté de l'Etat, il lui a été demandé en quoi la consultation par un particulier de son dossier individuel pouvait porter atteinte à la vie privée d'une tierce personne.

La réponse fut :

En consultant son dossier individuel, un particulier est susceptible de prendre connaissance, non

⁽³⁾ traduction libre

⁽⁴⁾ idem

seulement d'informations qui concernent sa propre personne, mais aussi d'informations qui concernent des personnes avec lesquelles il est en relation et qui doivent rester confidentielles.

La consultation d'un dossier individuel est également susceptible de fournir des informations de nature à en identifier la source.

En conclusions, le Comité R constate que la Sûreté a rejeté toutes les demandes de consultation qui lui ont été adressées parce que *“d'une part l'intérêt de la publicité ne l'emporte pas sur la protection de la Sûreté nationale (art. 6 § 1er, 4° de la loi du 11 avril 1994 relative à la publicité de l'administration) et que d'autre part, la consultation des documents administratifs demandés porte atteinte à la vie privée de tierces personnes ainsi qu'à une obligation de secret instaurée par la loi (art. 6 § 2, 1° et 2° de la loi précitée).”*⁽⁵⁾

L'administrateur général de la Sûreté de l'Etat signale toutefois aux demandeurs qu'il leur est loisible d'introduire une demande de reconsidération auprès de son Administration en même temps qu'une demande d'avis auprès de la Commission d'accès aux documents administratifs, conformément à l'article 8 § 2 de la loi du 11 avril 1994 relative à la publicité de l'administration.

6.2. L'application de ces législations par le SGR

Nombre de demandes introduites : en 1994, 3, en 1995, 44 et en 1996, 4.

Nombre d'acceptations : aucune

Nombre de refus : 51

Motifs :

Répondant à une demande de consultation portée à la connaissance du Comité R, le chef du SGR, a fait savoir au demandeur que *“contrairement aux dispositions relatives aux autres fichiers, le droit d'accès et de rectification à l'égard des fichiers du SGR par une personne privée est exercé par l'intermédiaire de la Commission de la protection de la vie privée. (...) Par ailleurs, - ajoute la lettre- si vous vous sentez lésé par une action quelconque du SGR, je suggère de vous adresser au Comité Permanent de Contrôle des Services de Renseignements, (...)”*.

La gestion de cette problématique est confiée au Secrétariat Administratif et Technique (SAT) du cabinet de la Défense nationale. Ce secrétariat est chargé de la tenue d'un registre central reprenant toutes les demandes concernant l'envoi de documentation ou d'éventuelle décision de refus. Même la demande de reconsidération a toujours été rejetée.

Seule une demande de communication de l'organigramme du SGR a été envoyée sur avis de la Commission d'accès aux documents administratifs.

Au cours du temps les arguments sur base desquels un refus était opposé à chaque demande ont évolué.

a. Initialement, l'article 6, § 1, 4° et § 2, 3° de la loi du 11 avril 1994 était invoqué.

b. A la suite du refus du SGR de donner accès à leur dossier personnel, certains parlementaires ont demandé un avis à la Commission d'accès aux documents administratifs.

c. Cet avis précise que ce type de demande relève de la compétence de la Commission de la

⁽⁵⁾ traduction libre

protection de la vie privée, en raison du principe général de droit qui énonce “lex specialis derogat lex generalis”.

- d. Actuellement, la demande de consultation est refusée, après avoir sollicité la Commission d'accès aux documents administratifs. Il est fait systématiquement référence à la compétence de la Commission de la protection de la vie privée, dont l'adresse est donnée au requérant.

Le chef du SGR mentionne enfin qu'une requête est déposée devant le Conseil d'Etat. Elle concerne un refus du SGR de donner l'accès à un particulier à son dossier.

Conclusions sur l'application de ces législations par les deux services de renseignement

Tant la Sûreté de l'Etat que le SGR refusent à un particulier l'accès à son dossier individuel détenu par les services de renseignement.

6.3. L'application de ces législations par la Commission de la protection de la vie privée

En l'absence d'arrêté royal d'application de l'article 13 de la loi du 8 décembre 1992, la Commission s'est déclarée, dans un premier temps, dans l'incapacité d'exercer la mission qui lui est confiée par l'alinéa 1, 2° de cet article.

Une série d'arrêtés royaux ont été pris en application de la loi du 8 décembre 1992, mais aucun d'eux ne concerne le droit d'accès et de rectification indirect dont il est question ici.

En novembre 1996, la Commission a déjà reçu plus de 45 demandes d'accès aux dossiers de la Gendarmerie, de la Sûreté de l'Etat et de la Police judiciaire.

Le Comité R renvoie le lecteur à la jurisprudence de la Commission de la protection de la vie privée en ce qui concerne l'application de l'article 13 alinéa 2 de la loi du 8 décembre 1992. Cette jurisprudence ne donne pas un accès direct aux particuliers aux données à caractère personnel détenues par les services de renseignement. La Commission de la protection de la vie privée informe les intéressés qu' "il a été procédé aux vérifications nécessaires" mais qu'ils ne peuvent être informés du contenu du dossier. La Commission consulte les dossiers sur place et demande aux services de renseignement de supprimer les données qu'elle estime ne pas devoir figurer dans ces fichiers. Selon le président de la Commission de la protection de la vie privée, les services obtempèrent (lettre du 29 octobre 1996).

6.4. L'application de ces législations par la Commission d'accès aux documents administratifs

Le président de la Commission d'accès aux documents administratifs a fait connaître la position de sa Commission. Celle-ci s'est exprimée dans cinq avis qui ont été rendus en 1994 et 1995 sur des demandes de particuliers. Ces avis s'énoncent comme suit :

“En vertu de l'article 13 de la loi du 8 décembre 1992, la Commission de la protection de la vie privée exerce le droit d'accès et de rectification indirect du particulier à l'égard des traitements automatisés et manuels de données à caractère personnel gérés par la Sûreté de l'Etat.

En principe, la loi précitée ne s'applique qu'aux fichiers et non aux dossiers. Cependant, la Sûreté de l'Etat ne disposant que d'un "fichier de référence" comportant les nom, prénom et numéro de dossier, le contrôle exercé par la Commission de protection de la vie privée sera étendu aux dossiers correspondants afin de vérifier l'exactitude des données et la pertinence de leur présence dans le fichier. (Doc. Chambre n° 413/12 - 91/92, p.16).

Il y a lieu de noter que les dossiers individuels de la Sûreté de l'Etat contiennent essentiellement des données à caractère personnel dites "sensibles" au sens des articles 6, 7 et 8 de ladite loi.

La compétence de la Commission de la protection de la vie privée à l'égard des traitements gérés par la Sûreté de l'Etat est exclusive conformément à l'article 3 § 3 alinéa 2 de la loi qui stipule que celle-ci est "seule compétente pour assurer l'exercice du droit d'accès et de rectification de la personne concernée conformément à l'article 13".

Les dispositions de cette législation sont plus strictes en matière de publicité des données. Il s'agit d'une législation spécifique qui déroge au principe général de la publicité instaurée par la loi du 11 avril 1994 et qui prévaut sur celui-ci. (Doc. Chambre n° 1112/13 - 92/93, p. 35).

En effet, l'art. 6, § 2, 2°, de la loi du 11 avril 1994 relatif à la publicité de l'administration stipule que l'autorité administrative fédérale ou non fédérale rejette la demande de consultation, d'explication ou de communication sous forme de copie d'un document administratif qui lui est adressée en application de la présente loi si la publication du document administratif porte atteinte à une obligation de secret instaurée par la loi.

En conséquence, la Commission d'accès aux documents administratifs estime que le droit d'accès aux dossiers individuels détenus par la Sûreté de l'Etat doit s'exercer via la Commission de protection de la vie privée, Rue de la Régence, 61, 1000 Bruxelles (Tél : 542.66.24)".

7. PROJETS ET PROPOSITIONS DE LOI INSTAURANT UN DROIT DE CONSULTER DES DOSSIERS DE LA SÛRETÉ DE L'ETAT

Sénat

- Une proposition de loi instaurant un droit à la consultation des dossiers de la Sûreté de l'Etat a été déposée le 25 juillet 1995 par Monsieur Verreycken (Vlaams Blok).

Monsieur Verreycken estime que la Sûreté de l'Etat menace la liberté d'expression en constituant des dossiers à propos des partis politiques, au nom de chaque mandataire et "*peut-être bien de tous les membres connus de ces partis*". Ce faisant, la Sûreté de l'Etat "*fournit ainsi à l'appareil judiciaire les moyens de réprimer les délits d'opinion*". Il convient donc de permettre aux intéressés eux-mêmes, par mesure de précaution et pour garantir le respect de la liberté d'opinion, de consulter les dossiers établis à leur nom et, le cas échéant, de réfuter ou de faire rectifier les informations fautives.

La proposition de loi prévoit que : "*Tout belge peut faire valoir son droit de consulter les dossiers que la Sûreté de l'Etat a établis à son nom*" et ce, quel que soit le support de l'information stockée. Ce droit est étendu aux héritiers jusqu'au second degré.

Cette proposition a été prise en considération le 12 octobre 1995 et renvoyée à la Commission de

la Justice. A ce jour elle n'a pas encore été discutée.

8. ACCÈS AUX DOSSIERS INDIVIDUELS VIA LE COMITÉ R

8.1. La loi organique du contrôle des services de police et de renseignements autorise-t-elle l'accès aux dossiers individuels via le Comité R ?

La loi organique du 18 juillet 1991 donne au Comité R la mission de garantir la protection des droits que la Constitution et la loi confèrent aux personnes. L'article 40 de cette loi charge donc le Service d'enquêtes du Comité R d'examiner les plaintes et dénonciations des particuliers qui ont été directement concernés par l'intervention d'un service de renseignement. Il faut ici qu'il y ait plainte ou dénonciation de la violation d'un droit. Dans ce cadre, les membres du Service d'enquêtes R font les constatations qui s'imposent (article 51). Ils peuvent notamment saisir tous objets et documents utiles pour leur enquête, à l'exception de ceux qui concernent une information ou une instruction judiciaire en cours. Dans ce cadre, il est possible que le Service d'enquêtes du Comité R saisisse des fichiers ou des dossiers individuels.

Un rapport final d'enquête est établi pour relater les actes d'enquêtes et rendre compte des conclusions que l'on peut en tirer. Ce rapport, confidentiel, est transmis au ministre compétent, aux chambres législatives et au président du Comité P (article 65 du règlement d'ordre intérieur).

Le Comité R peut aussi envisager de publier tout ou partie de ses rapports, à l'exception de certaines données confidentielles (article 66 du règlement d'ordre intérieur).

La philosophie générale de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements et le règlement d'ordre intérieur du Comité R indiquent que les données qu'il recueille sont classifiées en raison du secret qui repose sur les activités des services de renseignement.

A l'occasion de la publication du rapport annuel, le Comité R se doit d'assurer un équilibre entre deux impératifs :

- d'une part, la nécessité d'informer aussi complètement que possible les autorités législatives;
- d'autre part, la nécessité de ne pas désorganiser le fonctionnement des services de renseignement, de ne pas le priver de ses sources d'information, notamment étrangères et enfin de ne pas mettre en péril la vie privée et l'intégrité physique de personnes.

Il s'en déduit que les impératifs de confidentialité et de sécurité doivent largement être pris en compte.

La lecture de l'exposé des motifs du projet de loi organique du contrôle des services de police et de renseignement permet de mieux cerner le contenu de la mission du Comité R précisée à l'article 1^{er} de ladite loi :

"Le Comité permanent vérifie si les actions ou la façon de travailler des services de police et de renseignements ne portent pas atteinte, de façon disproportionnée ou injustifiée, aux droits et libertés ou ne révèlent un manque d'efficacité ou de coordination"⁽⁶⁾

⁽⁶⁾ Doc. Parl., Chambre, sess. o. 1990/1991, n°1305/8 p. 13, § 3)

C'est dans ce cadre que doit s'interpréter l'article 66, alinéa 5 du règlement d'ordre intérieur qui reconnaît *"le droit des plaignants de connaître la suite qui a été réservée à leur plainte."*

Ni la loi, ni le règlement d'ordre intérieur ne prévoient que le dossier d'enquête peut être communiqué au plaignant.

L'article 61 alinéa 3, du règlement d'ordre intérieur relatif à la communication des dossiers à la Chambre des Représentants et au Sénat stipule que :

"La décision de communication des dossiers ne peut être prise qu'à la majorité de quatre voix".

En conclusions, le Comité R estime que les dossiers individuels des services de renseignement contenus dans les dossiers d'enquêtes du Comité R sont confidentiels par nature. Ils ne peuvent être communiqués qu'au Parlement, à sa demande, et avec l'accord d'une majorité qualifiée de membres du Comité R. Cet accord est soumis à de strictes conditions destinées à garantir le secret d'informations sensibles. Ces dossiers ne peuvent jamais être communiqués aux plaignants.

8.2. La communication des rapports d'enquêtes

Les articles 33 et 35 de la loi organique du 18 juillet 1991 indiquent à qui, et dans quelles conditions, le Comité R dresse ses rapports d'enquêtes. Un rapport d'enquête a pour but de relater les actes d'enquêtes et de rendre compte des conclusions que l'on peut tirer en ce qui concerne les missions générales du Comité R (article 64 du règlement d'ordre intérieur).

Si, après enquête sur plainte d'un particulier, le Comité R parvenait à la conclusion que les droits que la Constitution et la loi confèrent à cette personne ont été violés par un service de renseignement, il n'est pas exclu que le rapport d'enquête mentionne certaines données personnelles contenues dans le dossier de l'intéressé.

Un rapport d'enquête est d'abord transmis aux ministres compétents et aux présidents du Sénat et de la Chambre des Représentants . Un tel rapport est confidentiel jusqu'à sa communication à la Chambre des Représentants et au Sénat.

En conclusion, le Comité R estime que le rapport d'enquête ne peut pas être communiqué au plaignant avant la décision du Comité R de le publier dans son rapport d'activités annuel.

8.3. Une possibilité, via le Comité R, serait ouverte par l'application de l'article 10 de la loi du 8 décembre 1992 relative à la protection de la vie privée

A l'heure actuelle, aucune disposition particulière n'écarte les comités P et R de l'application de l'article 10 de la loi du 8 décembre 1992 même lorsqu'ils traitent des données provenant des services de renseignement.

Cet article permet à toute personne d'obtenir communication des données qu'un traitement contient à son sujet. Par application de cet article 10, une personne pourrait demander communication des données que le Comité R possède sur elle. N'est-ce pas là une possibilité pour un plaignant de contourner un éventuel refus du Comité R de lui donner connaissance des suites de sa plainte ?

Pour résoudre ce problème, le Comité R a envoyé au ministre de la Justice le texte d'un projet de loi relatif à la modification des articles 3 et 13 de la loi du 8 décembre 1992 relative à la protection

de la vie privée à l'égard des traitements de données à caractère personnel. Cette proposition a pour objet de soumettre les traitements de données à caractère personnel, gérés par le Comité permanent de contrôle des services de renseignement et certains de ces traitements de données, gérés par le Comité permanent de contrôle des services de police, aux dispositions applicables aux traitements de données gérés par les services de renseignement.

Le projet a été adressé au ministre de la Justice le 6 janvier 1995; ce dernier a chargé son administration de l'étudier.

Une proposition de loi modifiant la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement a été déposée le 17 juillet 1996 par le député R. Delathouwer et le 19 juillet 1996 par la sénatrice J. Milquet.

L'article 31 de cette proposition de loi répond à la préoccupation du Comité R énoncée ci-dessus. Cet article complète les articles 3 § 3 premier alinéa, l'article 11 et l'article 13 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

L'exposé des motifs en est le suivant :

“La loi du 8 décembre 1992 relative à la protection de la vie privée prévoit certaines modalités particulières pour le traitement des données à caractère personnel par les services de police et de renseignements. Il est proposé de soumettre les données à caractère personnel traitées par chaque comité et par son Service d'enquêtes au même régime légal que les données à caractère personnel gérées par les services de police et de renseignements.”⁽⁷⁾

Un exposé identique de s motifs se retrouve dans les documents parlementaires du Sénat.

Gageons qu'une réponse sera ainsi donnée aux préoccupations du Comité R en cette matière.

9. CONCLUSIONS

9.1. L'accès direct (loi du 11 avril 1994)

Actuellement un particulier n'a pas d'accès direct à son dossier individuel auprès d'un service de renseignement.

La Sûreté de l'Etat soulève, par principe, les exceptions prévues par la loi relatives à la sûreté nationale et à l'atteinte à la vie privée pour s'opposer à la demande d'un particulier de consulter sur place son dossier.

Le SGR estime quant à lui que l'accès d'un particulier à son dossier ne peut avoir lieu qu'indirectement. Il suggère au demandeur de s'adresser à la commission de la protection de la vie privée. En cas de plainte, ce service renvoie le plaignant au Comité R.

La commission d'accès aux documents administratifs considère quant à elle que la loi du 11 avril 1994 relative à la publicité de l'administration doit s'effacer devant la loi du 8 décembre 1992 sur la

⁽⁷⁾ Doc. parl Chambre, session ordinaire 1995-1996 -000/0-95/96 p. 6

protection de la vie privée à l'égard des traitements de données à caractère personnel qui en son article 13 donne compétence exclusive à la commission de la protection de la vie privée pour traiter ce type de demande.

Le Conseil d'Etat est compétent pour censurer un refus ou une absence de décision de la commission d'accès aux documents administratifs sur une "demande de reconsidération". A ce jour le Comité R ignore la jurisprudence du Conseil d'Etat en la matière, même s'il sait qu'un recours a été introduit récemment.

9.2. L'accès indirect (loi du 8 décembre 1992)

Le droit d'accès indirect à un dossier détenu par un service de renseignement existe via la commission de la protection de la vie privée. Comme indiqué ci-dessus, tant la Sûreté de l'Etat que le SGR font référence à la loi du 8 décembre 1992 dans les réponses qu'ils adressent aux particuliers. La commission consulte les dossiers détenus par les services de renseignement et fait procéder aux rectifications; elle fait uniquement savoir au demandeur qu'il a été procédé aux vérifications nécessaires.

9.3. L'accès par recours au Comité R (loi du 18 juillet 1991)

Le Comité R estime que les dossiers individuels des services de renseignement contenus dans les dossiers d'enquêtes du Comité R sont confidentiels par nature. Ils ne peuvent être communiqués qu'au Parlement, à sa demande, et avec l'accord d'une majorité qualifiée de membres du Comité R. Cet accord est soumis à de strictes conditions destinées à garantir le secret d'informations sensibles. Ces dossiers ne peuvent jamais être communiqués au plaignant. Le plaignant peut seulement prendre connaissance du rapport d'enquête que le Comité R décide de rendre public suite à sa plainte.

10. RECOMMANDATIONS

- 1) Le Comité R souhaite une transparence accrue en vue d'une meilleure protection des droits des particuliers.
Le Comité R préconise à cet égard une procédure et des conditions d'accès inspirées par les législations suisse et française.

Le Comité R estime qu'une personne qui fait état d'un préjudice matériel ou moral vraisemblable en rapport avec des informations contenues sur elle dans un dossier des services de renseignement devrait pouvoir obtenir, sous certaines conditions mais de manière plus large qu'aujourd'hui, un droit de consulter ces documents. L'opportunité de permettre ou de refuser cet accès ne doit pas être laissée à la seule appréciation des services de renseignement.

Un organisme collégial tel que le Comité R, après avoir pris l'avis du ministre compétent, pourrait constater que la communication de certaines informations ne met en cause ni la Sûreté de l'Etat, ni la défense et la sécurité publique ni la sécurité des particuliers. Dans ces cas, il y aurait lieu de les transmettre au demandeur selon l'une des procédures suivantes :

- l'organisme indique à l'intéressé que le service de renseignement sollicité ne détient aucune information le concernant;

- l'organisme communique à l'intéressé tout ou partie des informations le concernant détenues par le service de renseignement sollicité.

Ne pourraient jamais être communiqués :

- le nom des membres des services de renseignement chargés de collecter et de traiter les informations personnelles;
- le nom des personnes ayant fourni de bonne foi les informations au service de renseignement;
- des informations relatives à la vie privée de tiers;
- des informations pouvant mettre en danger l'intégrité physique de tiers;
- des informations recueillies dans le cadre d'une procédure judiciaire en cours;
- des informations communiquées par un service de renseignement ou de sécurité étranger. C'est surtout dans ce dernier cas que la compétence du Comité R s'impose.

Lorsque des raisons de sûreté de l'Etat, de défense nationale, de sécurité publique et de sécurité des particuliers s'opposent à la communication d'informations, l'organisme informe le requérant qu'il a été procédé aux vérifications nécessaires.

2) Le Comité R recommande le vote à brève échéance de l'article 31 de la proposition de loi déposée par le député R. Delathouwer et la sénatrice J. Milquet en juillet 1996. Cet article complète les articles 3 § 3 premier alinéa, l'article 11 et l'article 13 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

L'exposé des motifs de l'article 31 de la proposition de loi de Monsieur Delathouwer et de Madame Milquet énonce :

" Il est proposé de soumettre les données à caractère personnel traitées par chaque comité et par son service d'enquêtes au même régime légal que les données à caractère personnel gérées par les services de police et de renseignements."⁽⁸⁾

Cette proposition de loi rencontre les souhaits du Comité R qui avait adressé un projet identique au ministre de la Justice le 6 janvier 1995.

11. POINT DE VUE DU MINISTRE

"Le Comité R a donné connaissance au ministre de la Justice du présent rapport le 28 mars 1997. Par sa lettre du 16 avril 1997, le ministre de la Justice a communiqué au Comité R l'avant-projet de loi transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données. Cet avant-projet de loi tend à modifier certaines dispositions de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, notamment :

⁽⁸⁾ Doc. parl Chambre, session ordinaire 1995-1996 -000/0-95/96 p. 6

- l'article 3 § 3 en incluant le Comité R et son Service d'enquêtes parmi les services de renseignement et instances de sécurité dont les traitements de données à caractère personnel échappent à certaines dispositions de la même loi (article 4 de l'avant-projet de loi);
- l'article 13 en soumettant les traitements de données à caractère personnel du Comité R et de son Service d'enquêtes au droit d'accès et de rectification indirect par l'intermédiaire de la Commission de protection de la vie privée (article 18 de l'avant-projet de loi).

L'avant-projet a été transmis aux Présidents de la Commission parlementaire le 24 septembre 1997.

Ces dispositions de l'avant-projet de loi répondent tout-à-fait aux recommandations du Comité R. Cet avant-projet de loi a été approuvé par le Conseil des ministres le 7 mars 1997 et a été, entre-temps, transmis pour avis au Conseil d'Etat".

CHAPITRE 3 : APPLICATION DE L'ARTICLE 33 DE LA LOI ORGANIQUE DU 18 JUILLET 1991 PAR LES SERVICES DE RENSEIGNEMENT

Rapport sur l'application par les services de renseignement de l'article 33, alinéa 2 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement.

1. INTRODUCTION

Aux termes de l'article 33, alinéa 2 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement, les services de renseignement transmettent d'initiative au Comité R les règlements et directives internes ainsi que tous les documents réglant le comportement des membres de ces services. Le Comité R et le Service d'enquêtes des services de renseignement ont le droit de se faire communiquer les textes qu'ils estiment nécessaires à l'accomplissement de leur mission.

Chaque année, le Comité R fait rapport sur la manière dont les services de renseignement se sont acquittés de cette obligation légale au cours de l'année écoulée.

2. L'APPLICATION DE L'ARTICLE 33, ALINÉA 2 PAR LA SÛRETÉ DE L'ÉTAT

2.1. Les documents transmis d'initiative

Depuis le 14 juin 1996 ⁽¹⁾, l'Administrateur général de la Sûreté de l'Etat a transmis d'initiative au Comité R neuf notes internes. Il s'agit des documents suivants :

⁽¹⁾ Date du dernier envoi de documents par la Sûreté de l'Etat mentionnée dans le rapport d'activités du Comité pour l'année 1996.

RÉFÉRENCE DU DOCUMENT	DATE DU DOCUMENT	OBJET
note sans référence	09/09/1996	critères de sélection des dossiers individuels;
N.S. non numérotée	20/09/1996	organisation des services administratifs et communs;
N.S. non numérotée	13/11/1996	restructuration partielle des services extérieurs de la Sûreté de l'Etat - Secret;
N.S. non numérotée	14/11/1996	modification partielle des structures des services administratifs et communs;
Liste des sujets	14/10/1996	secret;
N.S. non numérotée	15/01/1997	adaptation du flux de données entre les bases de données des services extérieurs et la fonction registry de l'application centrale;
N.S. non numérotée	23/04/1997	contacts avec les différents corps de police;
N.S. non numérotée	05/05/1997	protocole d'accord avec le SGR
N.S. non numérotée	26/06/1997	communication d'informations aux instances officielles.

2.2. Les documents transmis sur demande du Comité

Dans le cadre de ses enquêtes, le Comité R s'est adressé au Secrétaire général du ministère de la Justice pour solliciter la communication de certains documents.

Par lettre du 6 février 1997, le Comité R lui a demandé s'il existait un arrêté royal fixant le cadre du personnel des services extérieurs de la Sûreté de l'Etat. Par sa lettre du 17 février 1997, le secrétaire général a répondu par l'affirmative et a communiqué au Comité R une copie de l'arrêté royal du 12 novembre 1993 *"portant fixation du cadre organique du personnel des services extérieurs de la section Sûreté de l'Etat de l'Administration de la Sûreté publique"*. Le secrétaire

général a fait savoir au Comité R que les arrêtés de cadre organique du personnel des services extérieurs de la Sûreté de l'Etat ne sont pas publiés au Moniteur belge.

Le Comité R regrette que cet arrêté royal, paru après son installation, ne lui ait pas été communiqué d'initiative.

2.3. Les documents dont la communication a été refusée au Comité

Aucun document sollicité par le Comité R à la Sûreté de l'Etat ne lui a été refusé au cours du dernier exercice.

2.4. La suite donnée par la Sûreté de l'Etat au rapport de 1996

Le chapitre 1 du titre II - *“nos services de renseignement - les études”* - du rapport d'activités de 1996 indique de quelle manière les services de renseignement se sont acquittés de cette obligation légale entre le mois de juin 1995 et le mois de juin 1996.

A propos de la Sûreté de l'Etat, les conclusions de ce rapport mentionnaient ⁽²⁾ :

“La Sûreté de l'Etat a omis de transmettre d'initiative plusieurs notes internes réglant le comportement des membres de ce service. Ce service a également refusé d'adresser au Comité R certains documents qu'il avait sollicités parce qu'il les estimait utiles à sa mission”.

Le Comité R a pris acte de ces faits en laissant juge le Parlement et les ministres compétents.

Le Comité R avait toutefois rappelé que le ministre de la Justice avait déclaré qu'il appartiendrait aux services de renseignement d'apprécier si un document règle le comportement des membres de ces services. Il avait aussi ajouté : *“Il est clair qu'en cas de doute, il y a lieu de communiquer les documents au Comité”* ⁽³⁾.

Invité à communiquer au Comité R ses observations sur le rapport de 1996, l'administrateur général de la Sûreté de l'Etat lui a écrit ce qui suit le 5 septembre 1996 :

“Les commissions parlementaires d'accompagnement ayant adopté un point de vue en la matière qui ne paraît pas être entièrement compatible avec le raisonnement développé dans l'annexe à votre lettre du 22 juillet 1996 - à savoir le projet de rapport -, j'ai fait parvenir quelques observations écrites à Messieurs les Présidents Swaelen et Delathouwer”.

Invité à communiquer au Comité R ses observations sur le projet du présent rapport de 1997, l'administrateur général de la Sûreté de l'Etat a transmis au Comité, le 9 septembre 1997, copie d'un échange de courrier datant du début de l'année 1996 entre lui et la Commission chargée du suivi parlementaire des Comités P et R. Dans sa lettre, l'administrateur général estimait que l'article 33 alinéa 2 de la loi du 18 juillet 1991 pouvait désormais être lu comme suit : *“Les services de renseignements transmettent d'initiative au Comité permanent R tous les ordres et notes de service*

⁽²⁾ Rapport d'activités de 1996, p. 24

⁽³⁾ Sénat - session de 1990 - 1991 - 9/7/91 - rapport fait au nom de la commission de l'Intérieur par M. Mouton - 1258/2, p. 57.

adressés à leur personnel". Les commissions lui ont répondu le 6 mai 1996 : "De commissies zijn van oordeel dat voormeld artikel niet extensief moet worden uitgelegd. Uit de parlementaire voorbereiding (inzonderheid het antwoord van de minister in stuk Senaat nr 1258/2 - 90-91, blz. 57) blijkt duidelijk welke draagwijdte volgens de wetgever aan het artikel toekomt"

(Traduction libre : "Les commissions estiment que l'article précité ne doit pas être interprété de manière extensive. Les travaux préparatoires parlementaires (en particulier la réponse du ministre au Sénat mentionnée dans la pièce n° 1258/2-90/91, page 57) font clairement apparaître la portée que le législateur accorde à cet article : "Il est clair qu'en cas de doute, il y a lieu de communiquer les documents au Comité R".

Il s'agit de la position exposée ci-dessus par le Comité R .

3. L'APPLICATION DE L'ARTICLE 33, ALINÉA 2 PAR LE SGR

3.1. Les documents transmis d'initiative

Depuis le 15 juillet 1996⁽⁴⁾, le chef du SGR a transmis d'initiative au Comité R les neuf documents suivants :

RÉFÉRENCE	DATE	OBJET
sans réf.	01/09/1996	règlement d'ordre intérieur du centre historique de documentation (SGR / CHD);
sans réf.	25/10/1996	aperçu des dispositions légales applicables aux agents civils du Service de sécurité militaire;
ORDRES PERMANENTS		
O.P. 00.00 à 13.11	19/11/1996	version française des O.P.
O.P. 20.02 à 24.01	28/11/1996	idem;
O.P. 30.02 à 31.01	10/12/1996	idem;
Note pour ...		
(SGR/ST/5051)	06/12/1996	réorganisation de la section SGR/ST;
O.P. 40.00 à 50	20/12/1996	version française des O.P.
N.S. SGR/S0050/97	06/03/1997	mouvements extrémistes et sectes (liste), Directives pour les différentes sections;
sans référence	20/02/1997	protocole d'accord entre le ministre de la Justice et le ministre de la Défense nationale

⁽⁴⁾ Date du dernier envoi de documents par le SGR mentionnée dans le rapport d'activités du Comité pour l'année 1996.

RÉFÉRENCE	DATE	OBJET
		réglant la coopération et l'échange d'informations entre la Sûreté de l'Etat et le SGRS.

3.2. Les documents transmis sur demande du Comité

Dans le cadre de ses enquêtes et de ses études, le Comité R s'est aussi adressé au ministre de la Défense nationale, à l'Administration générale civile du ministère de la Défense nationale, à l'Etat-major des forces armées et au SGR pour obtenir certains documents qu'il estimait utile à l'accomplissement de sa mission; il s'agit des documents suivants :

- la note intitulée "concept pour la défense militaire du territoire" (janvier 1997), de même que le projet de note controversée qui a donné lieu à l'enquête sur la création éventuelle d'un nouveau service de renseignement militaire;
- la décision du Comité ministériel de Défense du 9 octobre 1975 instituant un collège des responsables du renseignement;
- un aperçu des dispositions légales et réglementaires applicables aux agents civils du Service de sécurité militaire; la copie de certaines de ces dispositions et avis du conseil d'Etat;
- les principaux textes normatifs afférents à l'aptitude physique des militaires;
- le "livre blanc 1994" de la Défense nationale édité en application de la loi du 11 avril 1994 relative à la publicité de l'administration;
- deux notes du ministre de la Défense nationale (22 novembre 1994 et 30 septembre 1996) concernant l'application de la loi du 11 avril 1994 relative à la publicité de l'administration par le ministère de la Défense nationale;
- avis n° 13 du 14 février 1997 du bureau du Conseil de l'Egalité des chances entre hommes et femmes, concernant les femmes dans les forces armées;
- avis prononcé le 26 mars 1996 par la Commission d'accès aux documents administratifs sur des demandes d'accès de parlementaires à leurs dossiers auprès des services de renseignement;
- liste des dénominations et abréviations employées au SGR pour en désigner les services et les sections.

3.3. Les documents dont la communication a été refusée au Comité

Aucun document sollicité par le Comité R au SGR ne lui a été refusé.

3.4. La suite donnée par le SGR au rapport de 1996

Le rapport d'activités de 1995 avait recommandé que les ordres permanents du SGR soient rédigés

dans les deux langues nationales. Le rapport d'activités de 1996 signalait qu'en ce qui concerne la mise à jour et la traduction en français des ordres permanents, le chef du SGR avait donné des instructions afin de régler ce problème au plus vite, en fonction des priorités du service.

Le Comité R a constaté que les ordres permanents du SGR étaient à présent disponibles dans les deux langues nationales comme il l'avait recommandé en 1995.

4. CONCLUSIONS

Le Comité R reçoit régulièrement des règlements et directives internes des services de renseignement (Sûreté de l'Etat et SGR) ainsi que des documents réglant le comportement des membres de ces services. Le Comité R ne s'est heurté à aucun refus de délivrance de documents sollicités au cours de l'exercice écoulé.

Il subsiste cependant un malentendu persistant entre le Comité R et la Sûreté de l'Etat à propos de l'interprétation de l'article 33, alinéa 2 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement. Les autorités responsables n'ont pris aucune mesure pour résoudre ce problème d'interprétation de la loi. Le Comité R n'a d'autres ressources que de le constater et de le regretter.

TITRE II : NOS SERVICES DE RENSEIGNEMENT

DEUXIEME PARTIE : LES ENQUÊTES

A. A LA REQUÊTE DU PARLEMENT OU DES MINISTRES

CHAPITRE 1 : RADIOSCOPIE DU SGR

SECTION 1 : INTRODUCTION

1. SAISINE DU COMITÉ

1.1. Saisine par le ministre de l'Intérieur

Par lettre du 24 avril 1996, monsieur Vande Lanotte a prié le Comité R de bien vouloir ouvrir une enquête afin de vérifier la véracité de certaines affirmations parues, le jour même, dans le journal "De Morgen". Cet article intitulé "leger bespiedt op grote schaal burgers" fait état de la constitution d'un "nouveau réseau d'espionnage de l'Etat-major (een nieuw spionagenetwerk van de generale staf)" destiné à "infiltrer la vie civile (om overal in het burgerleven te infiltreren)" à partir des nouvelles sections du SGR établies dans tous les chefs-lieux de province. Toujours selon cet article, "Via betaalde informanten worden lijvige dossiers aangelegd over milieu-activisten en vredesmilitanten, allerhande minderheidsgroepen, sekteleiden en figuren uit de kriminaliteit".

1.2. Saisine par la Chambre des représentants

Par lettre du 2 mai 1996, monsieur Delathouwer, président de la Commission spéciale chargée de l'accompagnement parlementaire des comités permanents de contrôle des services de police et de renseignement a fait savoir à la présidente du Comité R, que la Chambre avait décidé d'émettre un avis favorable sur les demandes d'enquêtes suivantes et de les soumettre au Comité R :

Questions de M. Deleuze :

"Quelles sont les activités du service de renseignement de l'armée ? Ce service procède-t-il à des écoutes téléphoniques ou à l'interception d'ondes électromagnétiques ? Avec quels moyens ? A partir de quels lieux ? De quelle manière la décision prise par le gouvernement le 23 novembre 1990 de supprimer le réseau Gladio en Belgique fut-elle suivie ?"

Questions de M. Moureaux :

"Quelles sont les missions, les activités et les moyens d'action, encadrement et informateurs, de la section SGR/IH - section Humint ? Le service Stay Behind a-t-il été transféré en tout ou en partie à la section Humint ou à une autre ? Ceci tant au niveau des instructeurs que des informateurs ? Ces restructurations ont-elles été opérées avec l'accord de la hiérarchie militaire et administrative ? Celle-ci a-t-elle été complètement informée et de quelle manière ?"

Par même courrier, monsieur Delathouwer ajoute : *“Lors de la dernière réunion de la commission, il nous est revenu qu’une enquête aurait été ouverte par le Comité R sur l’article paru dans “De Morgen” du 24 avril 1996. S’il en est ainsi, la commission spéciale appuie cette initiative et demande qu’une enquête approfondie soit menée concernant toutes les matières soulevées dans la présente, et ce en les globalisant”.*

1.3. Saisine par le ministre de la Défense nationale

Par lettre du 13 mai 1996, monsieur Poncelet, ministre de la Défense nationale, fit savoir au Comité R qu’il avait annoncé à la Chambre des représentants qu’il le saisisait d’une demande d’enquête *“concernant la réorganisation et les activités des sections provinciales du SGR”.*

Ayant reçu depuis lors la notification de l’ouverture par le Comité R d’une enquête d’office sur ce sujet, le ministre de la Défense nationale a souhaité que celle-ci *“soit élargie aux motifs de la réorganisation et à la légalité des activités des sections provinciales”.*

2. OUVERTURE DES ENQUÊTES - PROCÉDURE

La demande d’enquête du ministre de l’Intérieur a été examinée par le Comité R lors de sa réunion du 25 avril 1996. Le Comité R a constaté que le ministre de l’Intérieur n’était pas l’un des *“ministres compétents”* qui, selon les termes des articles 31 et 32 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, pouvaient demander une enquête au Comité R. Après en avoir délibéré, le Comité R a néanmoins décidé à l’unanimité d’ouvrir une enquête d’initiative en raison des rumeurs courant sur les activités du SGR, des critiques répétées émises à l’égard de ce service et de son chef. Cette décision est mentionnée dans le procès-verbal de la réunion du Comité R tenue le 25 avril 1996. Elle a été notifiée le jour même à monsieur Vande Lanotte. La décision a été notifiée en termes généraux au Parlement et aux ministres compétents par lettres du 26 avril 1996. Il s’agit de l’enquête à laquelle monsieur Delathouwer fait allusion dans sa lettre du 2 mai 1996 citée au point 1.2. de ce rapport.

La requête introduite par la Chambre des représentants le 2 mai 1996 fut examinée par le Comité R en réunion du 9 mai 1996. Celui-ci a décidé, conformément au vœu de la Chambre, de traiter en une seule enquête les quatre demandes dont il était saisi à ce jour, à savoir celles qui concernent :

- les activités du SGR en général;
- les éventuelles écoutes téléphoniques et l’interception d’ondes électromagnétiques;
- la reconstitution éventuelle d’un réseau *“stay behind”* autrefois connu sous le nom de *“réseau Gladio”* sous le couvert de la section *“Humin”* du SGR;
- la création de cellules provinciales par le SGR et leurs activités à l’égard des civils.

Il fut décidé que les quatre membres du Comité R participeraient ensemble au déroulement de cette enquête.

Le 15 mai 1996, le Comité R a notifié l’ouverture de l’enquête au Parlement; il a fait savoir au ministre de la Défense nationale que sa demande complémentaire introduite le 13 mai 1996 était intégrée aux enquêtes ouvertes les 25 avril 1996 et 9 mai 1996.

Le 23 mai 1996, le Comité R a notifié l'ouverture de l'enquête au ministre de la Justice.

3. QUESTIONS PARLEMENTAIRES DÉJÀ POSÉES SUR LES SUJETS DE L'ENQUÊTE DU COMITÉ R

Le Comité R a pris connaissance des questions parlementaires suivantes déjà posées sur les sujets de l'enquête. Certaines réponses livrent quelques éléments intéressants pour l'enquête du Comité R.

3.1. Questions posées au sujet du réseau "Stay behind"

La question n° 858 du député Vanhorenbeek (VU) au ministre de la Défense nationale le 13 juin 1991 porte sur la dissolution de la section SDRA VIII du SGR.

Réponse : *"SDRA VIII était la section du SGR chargée de la préparation d'un réseau clandestin pouvant être activé en cas d'une occupation ennemie du territoire national. En novembre 1990, le ministre de la Défense nationale a donné l'ordre de dissoudre SDRA VIII et la section a définitivement cessé d'exister le 1er janvier 1991".*

3.2. Questions posées au sujet de la constitution de cellules provinciales par le SGR

La question n° 251 du député Olivier Deleuze (Ecolo) le 18 février 1997 porte sur la tenue des enquêtes dont il est fait ici rapport.

3.3. Questions posées au sujet des écoutes téléphoniques et de l'interception de télécommunications

Dans son rapport général d'activités de 1996, le Comité R cite neuf questions parlementaires au sujet d'écoutes auxquelles procéderaient les services de renseignement ⁽¹⁾ :

- la question n° 94 de M. Tobback (SP) au ministre de la Défense nationale le 19 janvier 1984;
- la question n° 46 de M. Van Dienderen (AGALEV) au ministre de la Défense nationale le 18 mars 1988;
- la question n° 21 de M. Eerdeken (PS) au ministre de la Justice le 17 juin 1988;
- la question du sénateur Coveliers (VLD) au ministre de la Défense nationale le 12 octobre 1995;
- la question du député Deleuze (ECOLO) au ministre de l'Intérieur le 26 octobre 1995;

⁽¹⁾ Le Comité R ne cite pas ici les questions et interpellations relatives aux écoutes judiciaires.

- la question du député Van Gheluwe (SP) au ministre de la Défense nationale le 9 novembre 1995;
- la question du député Deleuze (ECOLO) au ministre des Télécommunications le 1^{er} décembre 1995;
- la question du sénateur Anciaux (VU) au ministre de la Justice le 16 janvier 1996;
- la question du sénateur Erdman (SP) au ministre de la Justice le 16 avril 1996.

A ces questions, il convient d'ajouter plus récemment l'intervention du député Lozie (AGALEV) à l'occasion de l'interpellation du ministre de la Justice par M. Moerman (PRL-FDF) (Chambre, SO 1996/1997 - Compte rendu analytique - COM 14.04.97).

Des réponses que le ministre de la Défense nationale a donné à ces différentes questions, il ressort que :

- les moyens et sources d'information du service de sécurité militaire ne sont pas communiqués;
- il existe à Peutie un centre de radio-transmissions de l'Etat-major, et non un centre d'interception de télécommunications;
- le chef du SGR a fait des propositions afin de permettre à son service de fonctionner;
- en ce qui concerne le respect des droits de l'homme, les militaires sont davantage que les "simples" citoyens, tenus au respect de certaines dispositions, étant donné qu'ils disposent de la force";
- le gouvernement prépare un projet de loi organique des services de renseignements;
 - le gouvernement prépare également un projet de loi modifiant la loi du 30 juin 1994 sur les écoutes téléphoniques.

SECTION 2 : LES ACTIVITÉS DU SGR EN GENERAL

1. APERÇU HISTORIQUE

C'est en 1915, durant la première guerre mondiale, qu'a été créé un "Service de Sûreté de l'Armée" (arrêté royal du 1^{er} avril 1915) et "*mis en place pour toute la durée de la guerre*".

Au fil des années, ce service s'est vu à plusieurs reprises restructuré; notamment durant la deuxième guerre mondiale (voir rapport d'activités du Comité "R" - 1995 - Titre 1 - Chapitre. 1 - p. 6).

Jusque dans les années 1960, les compétences du service de renseignement et de la Sûreté militaire étaient basées sur l'arrêté royal du 27 mai 1937 et sur l'arrêté du régent du 23 février 1947.

L'arrêté royal du 3 décembre 1963 déterminant la structure générale du ministère de la Défense nationale et des forces armées dispose en son article 23 § 2 b "*que le chef de l'Etat-major est entr'autres responsable de la recherche, de l'exploitation et de la diffusion du renseignement ainsi que de l'application des règles de la sûreté militaire et du contre-espionnage*".

Cet arrêté royal a lui-même connu plusieurs adaptations.

En 1989 l'arrêté royal du 19 décembre 1989, portant organisation de l'Etat-major général décrit comme suit les missions actuelles du SGR :

- la recherche, l'exploitation et la diffusion du renseignement;
- la prise de toutes mesures nécessaires à la protection du secret et au maintien de la sécurité militaire, y compris le chiffrement ainsi que l'établissement, la diffusion et le contrôle des directives en cette matière;
- la gestion des relations avec les autres services de renseignement et de sécurité, belges et étrangers;
- le respect des accords internationaux conclus par la Belgique en matière de sécurité;
- l'établissement, la diffusion et le contrôle des prescriptions relatives aux archives et à la documentation historique des forces armées (armée, gendarmerie).

2. ACTIVITÉS ACTUELLES DU SGR

Le commandement du service : le chef du SGR (actuellement un général major) est placé sous l'autorité directe du chef d'Etat- major général.

Il est chargé, d'une part, de la recherche, de l'exploitation et de la diffusion du renseignement d'ordre militaire, géographique, économique et politique.

Il est, d'autre part, chargé de prendre toutes les mesures nécessaires à la protection du secret et au maintien de la sécurité militaire ainsi que d'établir, diffuser et contrôler les directives en cette matière.

Outre ces deux missions principales, le chef du SGR assure les responsabilités suivantes :

- il gère les relations avec les forces armées étrangères. Ces relations sont principalement établies par la voie des attachés militaires belges en poste à l'étranger ainsi que des attachés militaires étrangers accrédités en Belgique;
- il assure les relations avec les autres services de renseignement et de sécurité nationaux et interalliés;
- il veille au respect des accords internationaux conclus par la Belgique en matière de sécurité;
- il établit, diffuse et contrôle les prescriptions relatives aux archives et à la documentation historique des forces armées.

En outre, le chef du SGR est responsable vis-à-vis du chef de l'Etat-major général du respect de l'ordre juridique, national et international, ainsi que des directives gouvernementales se rapportant aux activités de son service.

Les activités du service

Le SGR comprend trois services principaux (Renseignements - Sécurité - Centre de documentation historique).

Ces trois services sont eux-mêmes subdivisés en sections.

2.1. Service Renseignement

Ce service comprend trois sections :

2.1.1. Section "exploitation du renseignement"

Dans le cadre de la politique du renseignement, des zones d'intérêts pour la Belgique et des priorités fixées par le chef de l'Etat-major général, cette section formule les "objectifs du Renseignement" qui définissent les domaines et les priorités pour la recherche des informations. Le service d'exploitation est chargé de l'étude de ces informations, de leur analyse et d'établir des synthèses sur les différents sujets traités. Ces synthèses sont diffusées aux autorités nationales concernées par la politique de défense de la Belgique ainsi qu'aux grands commandements militaires, à l'OTAN, au SHAPE et éventuellement à certains services de renseignement étrangers amis, pour autant que les intérêts nationaux le permettent.

2.1.2. Section "recherche du renseignement" (HUMINT)

Cette section a pour but de rechercher des informations dans les limites fixées par le chef du SGR en se basant sur les éléments résultant des analyses de la section "exploitation".

Ces recherches sont axées vers l'extérieur du pays et exploitent tant les sources ouvertes que fermées.

Ces informations sont appelées "humint" du terme anglais "human intelligence" car elles sont recueillies par des moyens humains.

2.1.3. Section “recherche du renseignement” (COMINT)

Cette section est chargée de la recherche et de l'analyse du renseignement. “Comint” est une abréviation anglo-saxonne pour désigner les “communications intelligence”

Ce type d'activité est principalement orienté vers le domaine militaire.

Etant donné les moyens nationaux réduits et l'absence de réglementation en Belgique en matière de captation d'ondes électromagnétiques, cette section travaille en étroite collaboration avec les services alliés analogues.

2.2. Service “Sécurité”

Le service sécurité a pour tâche générale d'assurer la protection de toutes les “matières” classifiées contre toute menace pouvant apparaître sur le territoire national ou être dirigée contre des unités belges déployées à l'étranger.

La notion de “matière” concerne les installations, les documents, les équipements et le personnel.

Les menaces principales contre lesquelles la sécurité doit réagir sont l'espionnage, le terrorisme et la subversion.

2.2.1. La section “sécurité militaire” (SGR/SMI)

Cette section est responsable, préventivement :

- de l'établissement des directives de sécurité d'application au sein des forces armées;
- de l'enquête sur d'éventuels incidents de sécurité pouvant survenir dans les domaines énoncés ci-avant;
- du contrôle du respect des directives de sécurité par la voie d'inspections, tant dans le cadre national que dans une optique OTAN ou UEO en ce qui concerne les départements de l'armée traitant des documents émanant de ces organisations.
- de fournir aux firmes qui en font la demande les normes auxquelles elles doivent souscrire pour obtenir une agrégation correspondant au degré de classification requis pour les matières qu'elles traiteront;
- de conseiller les firmes dans la réalisation de ces normes;
- de contrôler leur bonne exécution avant l'agrégation officielle;
- d'assurer par la suite leur maintien par des inspections régulières.

Cette section a également pour mission de contrôler l'application des règles relatives la consultation et à l'utilisation de brevets belges et étrangers.

2.2.2. La section “habilitation et documentation”

Cette section a pour mission la délivrance des habilitations de sécurité tant pour le personnel de la Défense nationale que pour celui de l'industrie.

2.2.3. Le détachement de gendarmerie

Etant donné que les deux sections de sécurité militaire et industrielle ne possèdent pas les moyens opérationnels ni les organes de recherche nécessaires à l'accomplissement de leurs enquêtes de sécurité, celles-ci sont menées par un détachement de gendarmerie placé sous les ordres du chef de la sécurité.

2.2.4. La section "contre-ingérence"

Elle a pour mission principale de rechercher activement et d'identifier toute menace contre la sécurité militaire en matière de sabotage, d'espionnage, de subversion ou de terrorisme. Cette section est chargée de renseigner les autorités responsables de ladite menace et de prendre ensuite les mesures de neutralisation adaptées.

Ces menaces peuvent émaner d'horizons les plus divers (groupuscules nationaux, organisations terroristes étrangères établies illicitement sur le territoire).

Lorsque l'activité de contre-ingérence, en principe limitée au domaine militaire, touche le domaine civil, il y a coordination avec la Sûreté de l'Etat.

2.2.5. La section "technique"

Cette section a pour missions principales :

- proposer la politique des forces armées belges pour la sécurité des communications et du traitement automatisé des informations ainsi que pour la protection contre l'écoute;
- rédiger les règlements, normes et directives pour la réalisation de la politique en matière de sécurité des communications et du traitement automatisé des informations, ainsi que pour la protection contre l'écoute et le contrôle de leur application;
- produire et distribuer les clés et documents cryptographiques nécessaires pour l'application des règlements, normes et directives en matière de sécurité des communications et du traitement automatisé des informations aux Forces armées et aux départements ministériels intéressés. (Ministère des Affaires étrangères, Justice, etc...)
- assurer les relations en matière de sécurité des communications et du traitement automatisé des informations avec les autres ministères et organismes gouvernementaux, avec l'industrie et éventuellement avec les autres services de sécurité alliés, nationaux ou internationaux.

2.3. Le centre de documentation historique

Ce centre gère les archives historiques des forces armées. Ces archives peuvent moyennant certaines règles de sécurité, être consultées par des personnes et organismes privés qui en font la

demande.

2.4. La section “Gestion”

Il existe en outre au SGR un service “GESTION” qui assure la gestion du personnel, de la logistique, du budget et des transmissions.

SECTION 3 : LES ÉCOUTES TÉLÉPHONIQUES ET LES INTERCEPTIONS DE COMMUNICATIONS AUXQUELLES PROCÉDERAIT LE SGR

1. OBJET DE L'ENQUÊTE

Les questions posées le 2 mai 1996 par le Parlement étaient les suivantes :

1. Le SGR procède-t-il à des écoutes téléphoniques ou à l'interception d'ondes électromagnétiques ?
2. Avec quels moyens ?
3. A partir de quels lieux ?

2. RÉTROACTES DE L'ENQUÊTE

La décision de mener une étude sur la législation en matière d'écoutes administratives avait été prise par le Comité R en date du 8 novembre 1995. Cette étude, parue dans le rapport d'activités du Comité R pour l'année 1996, a été menée suite à une série d'articles parus dans la presse, essentiellement flamande : ceux-ci dénonçaient de prétendues pratiques illégales de la part du SGR, et notamment l'interception de communications de civils et d'ambassades (voir ci-après). Dans ces articles, il est également question de surveillance d'organisations pacifistes et écologistes, de même que du maintien en activité d'une unité de "counter-intelligence" en Allemagne. L'étude préalable du Comité R n'aborde que le problème de la légalité des écoutes téléphoniques et des interceptions de communications par rayonnements électromagnétiques.

Les conclusions de cette étude sont : "Dans l'état actuel de la législation belge, les services de renseignements nationaux ne disposent donc d'aucune possibilité de procéder légalement à des écoutes ou à des interceptions de télécommunications privées, même militaires, même à l'étranger et même en temps de guerre".

L'étude a été soumise pour avis à monsieur Stefaan De Clerck, ministre de la Justice, à monsieur Jean-Pol Poncelet, ministre de la Défense nationale, au Général-major Georis, chef du SGR et à monsieur Bart Van Lijsebeth, administrateur général de la Sûreté de l'Etat.

Un échange de vues s'est déroulé à ce sujet le 10 mai 1996 avec monsieur le ministre de la Défense nationale.

Ce dernier a adressé le 15 mai 1996 une note au chef de l'Etat-major pour l'informer de la teneur des conclusions de l'étude du Comité R. Dans cette note, le ministre annonce le dépôt à la Chambre d'un projet de loi autorisant notamment "la captation, l'écoute, la prise de connaissance ou l'enregistrement par le SGR, à des fins militaires, de radiocommunications militaires émises à l'étranger". Et le ministre d'ajouter : "En attendant que le Parlement se prononce sur ce projet de loi, j'attire votre attention sur la nécessité de continuer à respecter les dispositions légales en vigueur. De plus, eu égard à l'impérieuse nécessité de protéger la sécurité de nos troupes engagées sur des théâtres d'opérations extérieurs, j'attire également votre attention sur le concept d'état de

nécessité⁽¹⁾ développé par la jurisprudence, en vertu duquel une infraction pourrait ne pas être sanctionnée par le juge au motif que la commettre était la seule manière d'éviter qu'il soit porté atteinte à une valeur supérieure à celle protégée par la disposition enfreinte". Copie de cette note a été adressée au Premier ministre ainsi qu'au Comité R.

3. LES ALLÉGATIONS DE LA PRESSE

La matière des écoutes téléphoniques a tenu la presse, tant néerlandophone que francophone, en haleine au cours du dernier trimestre de l'année 1995. Le Comité R a pris connaissance d'une série d'articles de presse dont il résulte que le SGR disposerait d'un centre d'écoutes à Peutie. En violation de la loi, des radio-communications ainsi que des conversations téléphoniques par mobiles y seraient interceptées; il serait même procédé à des écoutes d'ambassades. Ces écoutes seraient pratiquées à grande échelle à l'aide d'un système scanner et d'installations mobiles aussi bien à l'intérieur qu'à l'extérieur du pays. Le chef du SGR de l'époque, qui est ingénieur spécialiste en télécommunications, l'aurait admis au cours d'une réunion tenue au cabinet du Premier ministre, arguant que ces pratiques, nécessaires pour la sécurité des forces armées, ne tomberaient pas dans le champ d'application de la Convention de sauvegarde des droits de l'homme, ni de la loi sur la protection de la vie privée.

L'information initiale a été donnée par le journal "De Morgen" le 21 septembre 1995 sous la signature de Walter De Bock. Les autres journaux qui relatent l'affaire ne font que reprendre, amplifier ou commenter l'information initiale du "De Morgen". A noter toutefois que dès le 16 septembre 1994, dans un article consacré au SGR, le journal "Le Soir" mentionnait déjà la section COMINT ⁽²⁾ qui rassemble "les sources technologiques - observation des émissions radio par satellites ...". A partir du 24 novembre 1995, la presse annonce les intentions du gouvernement à propos de l'avant-projet de loi sur les services de renseignement, les écoutes téléphoniques et l'interception de communications par le SGR. Le 28 novembre 1995, "Le Soir" annonce déjà qu'une "information" est ouverte à l'Auditorat militaire et au Comité R.

Plus récemment, dans une interview qu'il a accordée à des "jeunes journalistes d'un jour", le chef du SGR répond à la question suivante : "Une polémique a récemment éclaté sur la question des écoutes radio que vous pourriez opérer à l'étranger. Est-ce une source importante ? Réponse : "Oui. Nous essayons toujours d'avoir un maximum de sources. Les communications en sont une ...". Cette interview est parue dans le journal "La Dernière Heure" le 26 septembre 1996.

4. QUESTIONS ET RÉPONSES PARLEMENTAIRES - DÉCLARATIONS OFFICIELLES DE MINISTRES

La série d'articles de presse citée plus haut a suscité quelques réactions parlementaires ⁽³⁾. Des réponses que le gouvernement a données à ces différentes questions et interpellations, il ressort que :

- les moyens et sources d'information du service de sécurité militaire ne sont pas communiqués

⁽¹⁾ Souligné par le Comité R

⁽²⁾ Dans le jargon du renseignement, le néologisme anglais "COMINT" vient de "COMmunication INTelligence", qui signifie "renseignements obtenus par surveillance des communications radio".

⁽³⁾ Comité R - étude sur la législation en matière d'écoutes administratives - rapport 1996 - p. 27.

publiquement;

- il existe à Peutie un centre de radio-transmissions de l'Etat-major, et non un centre d'interception de télécommunications;
- le chef du SGR a fait des propositions afin de permettre à son service de fonctionner; les déclarations attribuées par la presse au chef du service de renseignement ont été amplifiées et certains propos rapportés n'ont pas été tenus. Le ministre de la Défense nationale a dès lors réaffirmé sa confiance dans le chef du service de renseignement;
- en ce qui concerne le respect des droits de l'homme, les militaires sont davantage que les "simples" citoyens, tenus au respect de certaines dispositions, étant donné qu'ils disposent de la force;
- le gouvernement prépare un avant-projet de loi organique des services de renseignement;
- le sénateur Coveliers a été invité à visiter le centre de télécommunications de Peutie.

Le 12 octobre 1995, monsieur Poncelet a promis à monsieur Coveliers d'organiser une visite à Peutie. Le sénateur Coveliers a accepté l'invitation du ministre de la Défense nationale à visiter les installations de Peutie, mais il a demandé d'être accompagné par un spécialiste en équipement d'écoutes. A ce jour, cette visite n'a pas eu lieu.

5. L'ENQUÊTE DU COMITÉ R

Le Comité R a procédé au recensement de tous les documents en sa possession provenant du SGR. Il a notamment utilisé les directives internes du SGR qui lui ont été transmises spontanément par ce service en application de l'article 33 de la loi organique du 18 juillet 1991. Il a également utilisé tous les comptes-rendus de briefing donnés au Comité R par des responsables du SGR.

Le Comité R a aussi procédé à deux auditions du chef du SGR de l'époque. Il a fait procéder à un devoir d'enquête par son Service d'enquêtes.

5.1. L'audition du chef du SGR au siège du Comité R le 16 juillet 1996

Le chef du SGR, invité au Comité R le 16 juillet 1996, a répondu à une série de questions préparées par le Comité R.

Il en résulte que ce service dispose d'un matériel d'écoutes téléphoniques, mais qui n'est plus utilisé. Le SGR conserve ce matériel dans l'espoir qu'une loi soit votée, à brève échéance, et que cette loi l'autorise à procéder à des écoutes téléphoniques. A cette date, un avant-projet de loi est en discussion au sein du gouvernement.

5.2. Les notes internes du SGR

Le lendemain de cette audition, le chef du SGR a remis au Comité R une copie d'une note interne du 17 mai 1994. Cette note est signée par le chef du SGR de cette époque. Il est clairement exprimé dans ce document qu'il est interdit de procéder à des écoutes à l'insu et sans l'accord

expresse des participants à un entretien.

Ce document fait également référence à la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement ainsi qu'à la loi du 8 décembre 1992 relative à la protection de la vie privée et des données à caractère personnel.

Le chef du SGR a également remis au Comité R une directive interne du 6 mars 1995 par laquelle il confirme celle prise par son prédécesseur en date du 17 mai 1994.

A cette directive est jointe une analyse de la loi du 30 juin 1994 relative à la protection de la vie privée, contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées.

Par ailleurs, les ordres permanents du SGR décrivent la mission d'écoutes stratégiques de la section COMINT du SGR.

5.3. Les instructions de l'OTAN

Le chapitre 7 d'une instruction non classifiée de l'OTAN en cours d'élaboration est consacré à "l'electronic warfare (EW)". Ce document rédigé en anglais n'est pas classifié. Il a été communiqué au Comité R en application de l'article 33 de la loi organique du 18 juillet 1991.

Extraits significatifs du document :

"Electronic Warfare (EW) is defined as : 'military action involving the use of electromagnetic (EM) energy, including directed energy (DE), to exploit and dominate the EM spectrum or to attack an enemy. It encompasses the interception and identification of EM emissions, the employment of EM energy to reduce or prevent hostile use of the EM spectrum and actions to ensure its effective use by friendly forces'. (...).

EW is an integral part of all military operations. It is directly related to signals intelligence (SIGINT)⁽⁴⁾ (...). EW contributes to situation assesment and decision-making, and has a three-fold role in allied joint operations :

- a. Electronic Warfare Support Measures (ESM) is the exploitive arm of EM, and can be considered as electronic surveillance. It is primarily associated with activities related to the search for, interception and identification of EM emissions and location of their sources for the purpose of immediate threat recognition. ESM provides valuable information on an daversary's intentions, and contributes to intelligence collection, steerage for Electronic Contermeasures (ECM) operations, deception planning and platform self-protection. ESM are passive and can be used in peace, crisis and war. (...).*
- b. Electronic Contermeasures (ECM) are the offensive or attack components of EW, and are defined as the division of EW involving actions taken to prevent or reduce an adversary's effective use of the EM spectrum, through the use of EM energy. (...).*
- c. Electronic Protective Measures (EPM) involve actions taken to ensure friendly effective use of*

⁽⁴⁾ Dans le jargon du renseignement, le néologisme anglais SIGINT vient de "Signal INTelligence" et signifie "renseignement obtenu par la captation de signaux radio".

the EM spectrum despite an adversary's use or exploitation of EM energy. (...).

(...) ESM operations exploit intentional emissions such as radio or radar signals, or unintentional emissions such as those at infra-red frequencies made by, for example, a vehicle or exhaust plume. (...)”.

6. L'ENQUÊTE JUDICIAIRE ET LA SUSPENSION DE L'ENQUÊTE DU COMITÉ R

Au cours de l'entretien du 16 juillet 1996 avec le chef du SGR, le Comité R a appris que l'Auditorat militaire avait ouvert une enquête judiciaire sur base des articles parus dans la presse. En application de l'article 69 du Règlement d'ordre intérieur, la Présidente a pris la décision de téléphoner immédiatement à l'Auditeur militaire, afin de vérifier l'information que le Comité R venait d'apprendre.

L'article 69 du règlement d'ordre intérieur du Comité R prévoit : *“Lorsque à l'occasion d'une enquête de contrôle, un membre du Service d'enquêtes constate un crime ou un délit commis par un membre des services de renseignements, l'instruction judiciaire relative à ces faits prend la priorité sur l'enquête de contrôle. L'enquête de contrôle se poursuit le cas échéant, en ce limitant aux éléments qui sont nécessaires à l'accomplissement des missions du Comité R. Le chef du Service d'enquêtes en avise alors le magistrat responsable de l'enquête judiciaire.”*

L'Auditeur général près la Cour militaire a confirmé la déclaration du responsable du SGR.

L'enquête a en conséquence été suspendue le 16 juillet 1996.

Le 29 juillet 1996, l'Auditeur général près la Cour militaire, confirme par écrit à la présidente qu'une enquête judiciaire relative à des écoutes téléphoniques ainsi que d'interceptions d'ondes électromagnétiques est actuellement en cours.

Le 1^{er} août 1996, l'Auditeur général près la Cour militaire a porté à la connaissance du Comité R que cette enquête judiciaire avait été classée sans suite par son office.

Suite à ce courrier, la présidente s'adressa à l'Auditeur général près la Cour militaire afin de lui demander de pouvoir prendre connaissance, en application de l'article 38 de la loi organique du 18 juillet 1991 sur le contrôle des services de police et de renseignements, des pièces et des documents de l'instruction. Le 21 août 1996, l'Auditeur général fit savoir qu'il estimait ne pas pouvoir communiquer les pièces du dossier d'enquête en raison du caractère très confidentiel desdites pièces.

Les conclusions de l'Auditeur général sont les suivantes :

- “1. Geen vaststaand element laat toe te stellen, dat er wordt overgegaan door de dienst ADIV van het Ministerie van Landsverdediging tot strafbare af luisterpraktijken ;*
- 2. Buitenlandse radiocommunicaties worden beluisterd, die betrekking hebben enerzijds op de aanwezigheid van Belgische troepen tijdens buitenlandse operaties in NAVO-verband, anderzijds op de beweging van vreemde eenheden. Het gaat hier om NAVO-standaardmethoden teneinde de veiligheid van onze militairen te waarborgen. “*

L'Auditeur général ajoutait : *“Het is U bovendien waarschijnlijk bekend dat een wetsontwerp deze laatste praktijken eerstdaags officieel zou moeten goedkeuren“.*

7. REPRISE DE L'ENQUÊTE PAR LE COMITÉ R

En date du 7 novembre 1996, le Comité R a décidé de reprendre l'enquête qui avait été suspendue le 16 juillet 1996. Une apostille fut adressée au chef du Service d'enquêtes afin d'entendre, à nouveau, le chef du SGR.

7.1. L'audition du chef du SGR effectuée au siège du SGR le 8 novembre 1996

En exécution de l'apostille précitée, le chef du Service d'enquêtes, s'est rendu, le vendredi 8 novembre 1996, au siège du SGR, quartier Reine Elisabeth à Evere afin d'y procéder à l'audition demandée. Il était accompagné de deux membres du Comité R.

Question :

Le SGR dispose-t-il d'installations mobiles pour procéder à l'interception de télécommunications? Si oui, lesquelles ?

Réponse :

Le chef du SGR déclare d'emblée que le SGR ne procède pas à l'interception de communications téléphoniques, ni en Belgique, ni à l'étranger. Mais le SGR procède bien à l'interception de télécommunications émises par ondes électromagnétiques à l'étranger⁽⁵⁾, ceci afin de récolter des informations indispensables pour assurer au mieux la sécurité de nos soldats.

Au cours d'opérations militaires, n'importe quel poste radio peut être utilisé comme moyen d'écoute. Dans tout exercice ou toute opération militaire, on se met à l'écoute des liaisons radios de l'adversaire en se plaçant sur les mêmes fréquences d'émissions que lui. Chacun le sait, les liaisons radios sont un moyen de communication ouvert à tout le monde. Mais ce moyen n'est pas protégé, c'est pourquoi les communications militaires sont en général protégées par des moyens cryptographiques.

En Belgique, les stations d'écoutes du SGR ne répondent à aucun besoin militaire spécifiquement belge. Les renseignements obtenus par ces stations fixes sont d'ordre stratégique. Ils ne sont exploitables que dans le cadre d'une coopération internationale avec des pays alliés.

Depuis l'effondrement du bloc soviétique, on assiste à une réduction généralisée des activités SIGINT dans les services de renseignement des pays alliés (France, Grande-Bretagne, Etats-Unis). Cette réduction des activités à l'étranger n'a aucune influence sur les activités COMINT du SGR. Ce service essaie de développer sa capacité de projection et de déploiement à l'étranger.

7.2. Les constatations du Service d'enquêtes du Comité R

Le Comité R sachant par ailleurs qu'une section du SGR dispose d'un matériel d'écoutes téléphoniques, la présidente du Comité R a chargé le chef du Service d'enquêtes de s'informer plus

⁽⁵⁾ Souligné par le Comité.

en détail sur la nature de ce matériel, son utilisation, d'en faire l'inventaire et de faire rapport.

Le Service d'enquêtes s'est fait présenter ledit matériel ainsi que son inventaire et l'a fait photographier le 13 novembre 1996.

Le Service d'enquêtes s'est fait produire la farde dans laquelle sont conservés les bons d'utilisation du matériel d'écoutes téléphoniques. Aucune trace récente d'utilisation n'a été relevée. Ce matériel a servi pour la dernière fois en 1988 dans le cadre d'une affaire d'espionnage au profit d'une puissance étrangère.

A la demande du chef du SGR, le Service d'enquêtes du Comité R a pris possession le 2 juin 1997 du matériel d'écoutes téléphoniques se trouvant dans les locaux du SGR. Un inventaire de ce matériel a été établi. Le matériel d'écoutes téléphoniques a été transféré dans le coffre blindé du Comité R à la même date.

8. LES CAUSES DE JUSTIFICATION EN DROIT PÉNAL

Dans l'état actuel de la législation belge, les services de renseignements nationaux ne disposent donc d'aucune possibilité de procéder légalement à des écoutes ou à des interceptions de télécommunications privées, même militaires, même à l'étranger et même en temps de guerre.

L'étude du Comité R a fait apparaître que, même effectuées dans le cadre d'opérations militaires légitimes, les interceptions de télécommunications ennemies enfreignent l'article 111 de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques.

En tant qu'agents de la force publique ayant intentionnellement, à l'aide d'un appareil quelconque, écouté et pris connaissance de communications ou de télécommunications privées, les militaires concernés enfreindraient aussi l'article 259bis du code pénal.

A propos des militaires belges en mission à l'étranger, l'article 10 bis de la loi du 17 avril 1878 contenant le titre préliminaire du code de procédure pénale indique ce qui suit : *"Toute personne soumise aux lois militaires qui aura commis une infraction quelconque sur le territoire d'un Etat étranger, pourra être poursuivie en Belgique. Il en est de même des personnes qui sont attachées, à quelque titre que ce soit, à une fraction de l'armée se trouvant en territoire étranger ou de celles qui sont autorisées à suivre un corps de troupe qui en fait partie"*.

Les militaires qui procéderaient à des interceptions de télécommunications à l'occasion de missions à l'étranger seraient donc, en principe, passibles d'un emprisonnement de six mois à deux ans et d'une amende de cinq cent francs à vingt mille francs ou d'une de ces peines seulement pour avoir intercepté les télécommunications des forces armées étrangères.

Une telle application aveugle du droit pénal ne pourrait que heurter le sens commun de tout citoyen.

Le Comité R s'est donc penché plus avant sur la position prise par le ministre de la Défense nationale dans la note qu'il a adressée le 15 mai 1996 au chef de l'Etat-major de l'armée : *"eu égard à l'impérieuse nécessité de protéger la sécurité de nos troupes engagées sur des théâtres d'opérations extérieurs, j'attire également votre attention sur le concept d'état de nécessité développé par la jurisprudence, en vertu duquel une infraction pourrait ne pas être sanctionnée par le juge au motif que la commettre était la seule manière d'éviter qu'il soit porté atteinte à une valeur supérieure à celle protégée par la disposition enfreinte"*.

Le droit pénal prévoit en effet certaines causes justificatives qui neutralisent l'élément légal de l'infraction et, partant, affectent son existence. *“A travers les mécanismes propres à chacune d'entre elles, les causes de justification traduisent, sur le plan du droit positif, l'inadaptation ou l'inadéquation du droit pénal par rapport à l'état de la conscience sociale. A la nécessaire rigidité du droit pénal, elles apportent le tempérament des circonstances exceptionnelles”* ⁽⁶⁾.

Le code pénal admet certaines “causes de justifications” qui résultent soit de l'accomplissement d'un devoir (ordre de la loi et commandement de l'autorité), soit de l'exercice d'un droit (légitime défense). La doctrine et la jurisprudence admettent également l'“état de nécessité” où l'infraction commise apparaît comme socialement nécessaire ou, à tout le moins, indifférente.

L'ordre de la loi et le commandement de l'autorité.

L'article 70 du Code pénal prévoit qu'“*il n'y a pas d'infraction lorsque le fait était ordonné par la loi et commandé par l'autorité*”. Cette cause ne pourrait être retenue ici : même si une interception de communication était commandée par l'autorité, le fait est prohibé par la loi.

La légitime défense.

“En droit positif, la légitime défense trouve sa source dans les articles 416 et 417 du code pénal qui déterminent, respectivement, les cas et les présomptions de légitime défense. Si ces dispositions visent l'homicide, les blessures et les coups, dans la mesure où ce sont les formes les plus courantes de résistance à l'agression, il est unanimement admis, (...) que le champ d'application de la légitime défense ne se limite pas à ces infractions. Toute infraction que la personne attaquée est dans la nécessité de commettre pour assurer sa défense (...) est, théoriquement, susceptible d'être justifiée par la légitime défense. Par ailleurs, la légitime défense est inscrite dans la loi non seulement au profit de la défense personnelle mais encore de la défense d'autrui. L'ensemble de cette matière est dominée par l'appréciation en fait par les cours et tribunaux des conditions d'existence et d'exercice de la défense légitime” ⁽⁷⁾.

L'état de nécessité.

Cette cause de justification n'est consacrée comme telle par aucune disposition légale; il s'agit d'une construction jurisprudentielle. L'état de nécessité peut se définir comme la situation dans laquelle se trouve une personne qui n'a raisonnablement d'autre ressource que de commettre une infraction pour sauvegarder un intérêt égal ou supérieur à celui que cette infraction sacrifie ⁽⁸⁾. La valeur supérieure à invoquer ici pourrait être la sûreté extérieure du pays ainsi que la sécurité physique des militaires engagés dans des opérations.

Le Comité R n'a cependant pas connaissance de jugements reconnaissant ces causes de justification pour des interceptions de télécommunications effectuées à des fins de sécurité. Il ne peut donc préjuger de l'application éventuelle de ces principes à de telles circonstances puisqu'ils sont soumis à l'appréciation souveraine du juge.

⁽⁶⁾ Introduction au droit pénal - Fr. Tulkens et M. van de Kerkove - *Story scientia* 1993 p. 204.

⁽⁷⁾ Fr. Tulkens et M. van de Kerkove - op. cit. p. 206 et suiv.

⁽⁸⁾ Fr. Tulkens et M. van de Kerkove - op. cit. p. 213.

9. CONCLUSIONS

1. Il existe au SGR une section COMINT (= COMmunication INTelligence) dont les attributions consistent en la recherche, le traitement et la diffusion de renseignements et d'informations techniques obtenues en captant des rayonnements électromagnétiques émis par des stations radiophoniques étrangères et ce, en coopération avec des nations amies ⁽⁹⁾.
2. Les attributions de cette section COMINT sont fixées dans les ordres permanents du SGR. Pour procéder à cette mission, le SGR se réfère également à une instruction non classifiée en cours d'élaboration à l'OTAN et qui est consacrée à l' "electronic warfare (EW)".
3. Ce type d'activité est essentiellement orienté vers le domaine militaire et permet, entre autres, de déceler la présence - ou la disparition - de grandes unités. La section COMINT travaille en étroite collaboration avec les services alliés analogues. Cette section reçoit également des services alliés des renseignements indispensables à la mise en état opérationnel d'équipements de sécurité.
4. A cette fin, le SGR dispose des moyens nécessaires. Pour des raisons de sécurité, le Comité R estime ne pas pouvoir révéler les lieux et le matériel utilisés pour ces opérations.
5. Le centre de Peutie ne dépend pas du SGR, il n'est pas un centre d'écoutes mais un centre de transmissions militaires à longue portée.
6. Ayant pris connaissance de l'étude que le Comité R a effectué sur les "écoutes administratives" (rapport d'activités 1996), le SGR est parfaitement conscient de l'absence de base légale pour procéder à ce genre d'opérations. Le chef du SGR a informé le ministre de la Défense nationale des problèmes que rencontre son service dans le cadre de la législation actuelle sur les écoutes et interceptions de télécommunications.
7. Eu égard à l'impérieuse nécessité de protéger la sécurité de nos troupes engagées sur des théâtres d'opérations extérieurs, le ministre de la Défense nationale a attiré l'attention du chef d'Etat-major sur le concept d'état de nécessité développé par la jurisprudence. En vertu de ce principe, une infraction pourrait ne pas être sanctionnée par le juge au motif que la commettre était la seule manière d'éviter qu'il soit porté atteinte à une valeur supérieure à celle protégée par la disposition enfreinte. Le Comité R ne peut toutefois préjuger de l'application éventuelle de ce principe à de telles circonstances puisqu'il ressort de l'appréciation souveraine du juge.
8. Une section du SGR dispose d'un matériel d'écoutes téléphoniques. L'utilisation de ce matériel est très strictement contrôlée. Celui-ci a été utilisé autrefois à des fins de contre-espionnage. Vu l'état actuel de la législation, ce matériel n'est plus utilisé. Plusieurs notes internes du SGR prohibent d'ailleurs le recours à cette méthode. Le Comité R et son Service d'enquêtes n'ont recueilli aucun élément, ni aucun indice permettant d'affirmer que le SGR a procédé récemment à des écoutes téléphoniques sur le territoire belge.
9. En 1996, l'Auditorat général près la Cour militaire a procédé à une enquête judiciaire relative à des écoutes téléphoniques ainsi qu'à l'interception d'ondes électromagnétiques par le SGR. Cette enquête judiciaire a été classée sans suite.

⁽⁹⁾ Souligné par le Comité.

10. Un projet de loi sur les services de renseignement a été déposé devant la Chambre des Représentants : ce texte prévoit notamment l'autorisation pour le SGR de capter des communications radio militaires émises depuis l'étranger.

11. Le matériel d'écoutes téléphoniques du SGR a été transféré le 2 juin 1997 dans le coffre blindé du Comité R.

10. RECOMMANDATIONS

Le Comité R rappelle qu'il s'est prononcé⁽¹⁰⁾ pour une seule loi spécifique réglementant toutes les formes d'interception de télécommunications, sous quelque forme que ce soit (paroles, signaux électriques, électroniques, etc ...) et véhiculées par quelque moyen technique que ce soit (par fils, ondes hertziennes, fibres optiques, etc ...) ainsi qu'éventuellement l'interception du courrier. Cette loi particulière serait applicable à tous les services légalement habilités à procéder aux interceptions de sécurité.

Le Comité R recommande que le projet de loi sur les écoutes administratives soit voté le plus rapidement possible par le législateur en tenant compte des six remarques formulées dans le rapport précité du Comité R⁽¹¹⁾ à ce propos :

- l'aspect législatif,
- l'adéquation des moyens aux finalités,
- les autorités responsables,
- les modalités de contrôle à mettre en oeuvre avant, pendant et après l'exécution de ces missions,
- le caractère non-judiciaire des écoutes de sécurité,
- les sanctions pénales.

⁽¹⁰⁾ Rapport d'activités du Comité R 1996, p. 49

⁽¹¹⁾ Idem p. 26 à 47

SECTION 4 : LA REINSTITUTION DU RESEAU STAY-BEHIND

1. OBJET DE L'ENQUÊTE

Les questions posées le 2 mai 1996 par le Parlement étaient les suivantes :

1. De quelle manière la décision prise par le gouvernement le 23 novembre 1990 de supprimer le réseau Gladio en Belgique fut-elle suivie ?
2. Quelles sont les missions, les activités et les moyens d'action, encadrement et informateurs, de la section SGR/IH - section Humint ?
3. Le service Stay-Behind a-t-il été transféré en tout ou en partie à la section Humint ou à une autre ?
4. Ceci tant au niveau des instructeurs que des informateurs ?
5. Ces restructurations ont-elles été opérées avec l'accord de la hiérarchie militaire et administrative ?
6. Celle-ci a-t-elle été complètement informée et de quelle manière ?

2. LES ALLÉGATIONS DE LA PRESSE

Tant la presse francophone que néerlandophone, ont régulièrement fait paraître des articles sur cette matière depuis le mois de septembre 1994.

Le Comité R a pris connaissance d'une série d'articles dont il résulte que le réseau dit "Gladio" resterait actif en Belgique.

Le 28 mars 1996, le journal "La Lanterne" a fait paraître un article suivant lequel *"le député socialiste Serge Moureaux l'affirme : le réseau clandestin de résistance n'a pas été dissout"*. Le 24 avril 1996, Walter De Bock écrivait dans "De Morgen" que le SGR avait mis en place un nouveau réseau, en redéployant des cellules provinciales. D'autres journaux ont relayé cette information.

Dans un article paru le 3 juin 1997 dans le journal "Le Soir" sous la plume de René Haquin, le juge Pierre Hennuy actuellement à la retraite, aurait déclaré à la commission d'enquête "bis" sur les tueries du Brabant wallon qu'en ce qui concerne la piste Gladio, l'enquête judiciaire n'a pas pu confirmer *"les déclarations d'un prétendu colonel américain sur une filière du Stay-Behind utilisée pour l'évacuation des tueurs"*.

3. MÉTHODOLOGIE

Le Comité R et/ou son Service d'enquêtes ont entendu le chef actuel du SGR, son prédécesseur, un premier sergent attaché à la section IH du SGR, le colonel responsable du SGR au moment de sa dissolution (actuellement à la retraite), le chef du SGR de 1986 à 1991 (également à la retraite), trois militaires de carrière affectés à la section IH du SGR.

La présidente du Comité R et le Service d'enquêtes ont également recueilli des informations auprès de diverses personnes.

Des constatations et vérifications ont été effectuées par le Service d'enquêtes dans les locaux occupés par le SGR. Les auditions (trois fardes) consignées lors de l'enquête parlementaire sur

l'existence en Belgique d'un réseau de renseignement clandestin international ont été consultées.

4. HISTORIQUE DU RÉSEAU STAY-BEHIND

Avant de répondre aux questions posées par les parlementaires, le Comité R estime utile de rappeler ce que représentaient les réseaux Stay-Behind et d'en résumer la genèse pour la Belgique.

Les réseaux Stay-Behind constituaient des réseaux nationaux des pays alliés de la seconde guerre mondiale. Ils ont été mis en place au début de la guerre froide. C'est en effet en 1952 que le gouvernement belge, en application des accords pris avec les alliés, décida de mettre sur pied ce réseau de renseignement destiné à couvrir la Belgique en cas d'occupation par les pays du bloc de l'Est.

Ce réseau avait pour mission de couvrir la totalité du pays occupé et de donner des renseignements au gouvernement belge en exil. Les renseignements devaient porter sur la situation du pays occupé. Ce réseau était destiné à fournir des informations sur l'état de fonctionnement des industries, sur les moyens de transport, de communication et de télécommunication. Le but était de recueillir des informations sur les activités essentiellement économiques et sociales du pays. Cette mission était dévolue au service civil (Sûreté de l'état) dudit réseau.

Une section militaire du réseau a également été mise en place car il était essentiel qu'un gouvernement en exil n'ignore rien des forces d'occupation ennemies.

Les réseaux tant civil que militaire se composaient d'agents des services de renseignement et de civils (informateurs) disséminés sur le territoire belge. Ces derniers étaient dénommés agents clandestins.

Ce réseau dénommé Stay-Behind s'occupait en résumé de renseignement, d'infiltration et d'exfiltration. Il s'agissait d'un système basé sur la confiance réciproque des alliés; dans ce cadre, chaque pays du "club" organisait une chaîne de solidarité permettant notamment l'évasion de personnalités importantes du territoire belge occupé par l'ennemi (exfiltration).

Le rapport de l'enquête parlementaire sur l'existence en Belgique d'un réseau de renseignements clandestin international ⁽¹⁾ relate parfaitement l'historique de ce réseau international. Le Comité R se réfère à ce rapport en ce qui concerne cet aspect de l'enquête.

Le 23 novembre 1990, le gouvernement belge a décidé de supprimer ce réseau. Le 3 décembre 1990, les services belges de renseignement ont notifié le retrait de la Belgique aux services alliés.

Le texte de la décision gouvernementale du 23 novembre 1990 est le suivant :

"Le Conseil décide d'abroger les missions qui avaient été confiées en 1951 par le Comité ministériel de défense au SDRA-8 existant au sein des Services généraux de renseignements des Forces armées et au service spécial existant au sein de la Sûreté de l'Etat en exécution des accords MENSIES-SPAAK relatifs à la préparation d'organisations d'espionnage et d'action en cas de guerre, ainsi que de rapporter les notes signées en 1952 par les responsables politiques de

⁽¹⁾ Doc. parl. session de 1990-1991 Sénat de Belgique 1117- 4 1990-1991 p. 17

l'époque concernant la coordination nécessaire entre ces services.

Il charge les ministres de la Justice et de la Défense nationale de l'exécution de cette décision.

Le Conseil décide en outre que notre pays informera de cette décision les autres pays parties aux accords précités.

Le Conseil décide enfin que le gouvernement apportera sa pleine collaboration à d'éventuelles commissions d'enquêtes parlementaires si les Chambres législatives décidaient d'en constituer.

Signé : *le secrétaire du Conseil*
 A. Alen"

5. SYNTHÈSE DE L'ENQUÊTE

5.1. Application de la décision gouvernementale du 23 novembre 1990 et participation de la hiérarchie militaire à cette décision

Le 28 mai 1996, le Comité R s'est adressé au ministre de la Défense nationale en lui demandant de pouvoir prendre connaissance des mesures prises par ses prédécesseurs, et adressées au chef de l'Etat-major général ou au chef du service de renseignement.

Le 19 juillet, le ministre a fort obligeamment transmis au Comité R une note émanant du chef de l'Etat-major à laquelle était annexée trois documents.

Le chef de l'Etat-major général dans sa réponse, communique au Comité R que la décision du Conseil des ministres du 23 novembre 1990 "est parvenue au chef du SGR par la voie du chef de l'Etat-major général".

Il ressort de la lecture de ce courrier que l'Etat-major n'a pu, malgré ses recherches, retrouver un document du ministre de la Défense nationale de l'époque, Guy Coëme, donnant des directives précises pour la dissolution du réseau dit "Gladio".

Seule une lettre du 27 mars 1991, émanant du ministre et adressée au colonel responsable du réseau Stay-Behind à cette date, précise que le ministre "est convaincu que SDRA-VIII n'a rien à se reprocher". Le ministre invite ce colonel à confier aux hauts magistrats désignés par la commission d'enquête parlementaire, toutes les informations dont il dispose, afin qu'à bref délai, il puisse être établi de façon indiscutable que l'honorabilité de tous ceux qui ont oeuvré pendant de longues années dans le cadre de la section SDRA-VIII ne pouvait être mise en doute.

La lecture du rapport de l'enquête parlementaire révèle que ce colonel n'a pas donné aux hauts magistrats toutes les informations qu'ils lui ont été demandées. Ainsi l'identité des agents clandestins du réseau n'a pas été communiquée aux magistrats.

Le 8 juillet 1996, le ministre de la Justice a donné connaissance au Comité R de la convention intervenue le 10 octobre 1991 entre l'administrateur de la Sûreté de l'Etat, et le chef du SGR, à propos de l'affectation au SGR du matériel de transmission du réseau Stay-Behind.

Cette note précise les mesures qui furent prises à l'occasion de la dissolution définitive du réseau.

Ces mesures ont été entièrement appliquées, écrit le ministre de la Justice. Ainsi tous les systèmes de radio communication furent transmis au ministère de la Défense nationale le 17 février 1993.

L'envoi de dix-neuf émetteurs récepteurs "harpoon", quarante batteries de réserve pour les harpoon et sept appareils de cryptographie a fait l'objet d'une convention signée par le chef du SGR à l'époque et l'administrateur général de la Sûreté de l'Etat à cette date.

La section SDRA-VIII (qui s'occupait de ce réseau) a été dissoute. Le personnel du SGR qui en faisait partie a, soit été muté dans d'autres unités de l'armée, soit été mis à la pension (les agents les plus âgés).

Les auditions du chef du SGR de 1986 à 1991 et du colonel responsable de la section SDRA-VIII au moment de sa dissolution peuvent être résumées comme suit :

Fin 1990, début 1991, une première décision de réduire le service de 50% des effectifs du SDRA-VIII a été prise par le général Charlier. En conséquence l'effectif des agents clandestins travaillant pour le SDRA-VIII a été réduit de 50%. Un agent qui n'est pas suivi devient rapidement inopérant. L'équipe n'était pas grande, elle se composait d'environ 40 personnes. Cette décision du général a été contestée et le colonel responsable de la section SDRA-VIII a écrit au ministre de la Défense nationale pour savoir si ce dernier marquait son accord à propos de cette décision. Ce colonel n'a jamais obtenu de réponse du ministre malgré une intervention de Monsieur Poswick ancien ministre de la Défense nationale et président du Comité de défense.

Les agents du SDRA-VIII ont été mutés ou mis à la pension. Les contractuels ont été remerciés, les officiers d'active, mutés et un soldat a été affecté à la section IH après avoir suivi un cours de sous-officier d'élite.

En avril 1991, la section a été supprimée. Le colonel responsable du réseau SDRA-VIII a pris sa pension.

Les agents clandestins en ont été avertis par leurs instructeurs, (les agents du SDRA-VIII). Ces derniers ont récupéré le matériel radio et des documents de systèmes de liaison ou codes de chiffrement.

Ce réseau n'avait pas de lien avec l'OTAN. L'organisation n'a jamais reçu de directives de l'OTAN ni d'instances civiles. Cependant il existait bien des contacts entre les différents pays ayant mis sur pied des réseaux de ce type en vue de leur coordination indispensable en cas d'exfiltration.

La décision gouvernementale belge a toutefois jeté un froid au sein des alliés de l'OTAN.

La Belgique en tant que responsable du secrétariat du réseau international Stay-Behind, représentait une plaque tournante des relations des services de renseignement des pays alliés.

Le colonel responsable du SDRA-VIII est passé à la réserve après sa mise à la pension sur avis favorable des cinq généraux des forces armées belges. Il avait gardé la confiance de sa hiérarchie. Ce colonel a déclaré ne plus avoir travaillé à partir de sa mise en pension, ni pour les services de renseignement belges ni pour les services de renseignement étrangers.

La hiérarchie militaire n'a pas été spécifiquement informée de la dissolution du réseau Stay-Behind, mais il va de soi qu'elle a été mise au courant des mutations et mises à la pension des agents de la section SDRA-VIII.

5.2. Les missions, activités, moyens, encadrement et informateurs de la section IH

5.2.1. Missions

Dans le cadre général des missions, classifiées secrètes, exercées par le SGR en application de l'arrêté royal du 19 décembre 1989, art. 14, par. 3, se trouve la recherche et la collecte d'informations non publiques à l'étranger au moyen de sources humaines, c'est-à-dire d'informateurs.

5.2.2. Activités

- L'organisation de la direction de la recherche des informations non publiques sur les zones et domaines tels que définis par le commandement du SGR.
- La recherche et la récolte d'informations non publiques à l'aide de sources humaines dans ces zones et domaines et selon les priorités qui sont principalement basées sur les besoins de la section exploitation du renseignement (SGR/IE).
- La transmission de ces informations aux instances compétentes du SGR.
- La gestion des sources propres et l'élaboration des mesures nécessaires à leur sécurité.
- Le maintien dans le cadre de sa mission des contacts avec certains services de renseignement étrangers.

5.2.3. Moyens

La section SGR/IH est composée d'agents, civils et militaires. Le nombre de ces agents est classifié secret. Elle dispose également de moyens de transmission d'informations.

Le Service d'enquêtes du Comité R a procédé à l'inventaire de ce matériel composé essentiellement d'émetteurs récepteurs, dénommés "harpoon", 68 appareils ont été identifiés. Un registre de sortie est tenu au sein de la section IH. Sur ces 68 harpoon, le Service d'enquêtes a dénombré 6 appareils en circulation.

Pour chaque appareil une explication a été fournie. La mise en fonction de ces appareils est justifiée par les missions actuelles du SGR.

5.2.4. Encadrement

La section IH est sous le commandement d'un Lieutenant Colonel, assisté de deux officiers adjoints.

5.2.5. Informateurs

Le nombre d'informateurs qui s'occupent de la recherche des informations ne peut être rendu public pour des raisons évidentes d'efficacité du service. Le Comité R renvoie à ce sujet le lecteur à

l'enquête menée sur cette problématique publiée dans son rapport annuel d'activités 1997⁽²⁾.

5.3. Le service Stay-Behind a-t-il été transféré en tout ou en partie à la section IH ou à une autre ? Ceci tant au niveau des instructeurs que des informateurs ?

La question a été posée au chef du SGR qui a répondu le 3 mars 1997 de la manière suivante:

“Le service Stay-Behind n’a ni en tout, ni en partie été transféré à la section SGR/IH ou à une quelconque autre section”.⁽³⁾

Le Service d'enquêtes et des membres du Comité R ont vérifié à l'occasion d'autres enquêtes, telles que les cellules provinciales, le CTI et les écoutes téléphoniques (enquêtes reprises dans la radioscopie du SGR à laquelle il a été procédé à la demande du Parlement) si des indices de la réinstauration de ce réseau Stay-Behind pouvaient être mis en lumière. Des constatations sur les lieux de travail du SGR ont été effectuées sans en avertir au préalable les responsables de ce service de renseignement et il a été procédé à l'improviste à des auditions approfondies des agents de ce service.

Aucun élément n'a été trouvé permettant d'affirmer que le réseau Stay-Behind a été transféré en tout ou en partie à la section Humint ou à une autre section du SGR.

Quant à la deuxième partie de la question, c'est-à-dire celle qui concerne le transfert des instructeurs et des informateurs, de plus amples explications sont indispensables, les données du dossier étant les suivantes :

Un premier sergent, a été affecté comme indiqué ci-dessus, à la section IH en qualité d'instructeur radio.

Ce premier sergent a commencé à travailler à la section SDRA VIII en 1988. A l'origine, il s'occupait de l'entretien et du saut en parachute. Il a ensuite été formé à l'utilisation du matériel de télécommunication utilisé par le SDRA-VIII. Ce matériel était constitué de “harpoon”, comme indiqué ci-dessus.

Ce type d'appareillage est conçu pour une utilisation clandestine. Il convient très bien pour des missions telles que celles confiées au réseau Stay-Behind. Ces appareils tout en étant encore partiellement utilisables, sont actuellement dépassés par les nouvelles technologies.

Des militaires de carrière ont été instruits par le premier sergent. Interrogées par le Service d'enquêtes du Comité R, ces trois personnes ont déclaré qu'aucune d'elle n'était chargée d'instruire des civils. L'enquête menée ultérieurement, n'a pas pu relever le moindre indice de réinstauration du réseau Stay-Behind. Ces radio opérateurs s'occupent de mettre sur pied le réseau vespa (autre dénomination du matériel harpoon) et d'en instruire le personnel organique et les collaborateurs militaires de la section SGR/IH.

Le Comité R n'a recueilli aucun indice indiquant que des informateurs de la section SDRA VIII auraient été transférés à la section Humint(IH). Cette hypothèse paraît peu plausible vu la

⁽²⁾ Rapport d'activités annuel du Comité R 1997 p. 134.

⁽³⁾ Traduction libre

différence essentielle qui existait entre les missions de l'ancien réseau Stay-Behind et celle de la section IH (*cf. point 5.2.2. du rapport d'enquête*).

Toutefois, il est impossible d'affirmer qu'aucun agent clandestin du réseau Stay-Behind n'est devenu informateur de la section IH, aucune identité n'ayant été communiquée.

6. AUTRES DEVOIRS D'ENQUÊTE

- a) Dans le cadre des enquêtes sur le commandement territorial interforce, les cellules provinciales et sur les écoutes téléphoniques, le Comité R n'a découvert aucun élément permettant d'affirmer qu'un nouveau réseau Stay-Behind a été mis sur pied.
- b) A la lecture des auditions effectuées par la commission d'enquête parlementaire sur l'existence en Belgique d'un réseau de renseignement clandestin international, le Comité R s'est demandé si une structure parallèle au réseau Stay-Behind n'avait pas subsisté au travers de certaines organisations mentionnées dans ce rapport d'enquête parlementaire.
Suite aux vérifications effectuées par le Service d'enquêtes, le Comité R n'a trouvé aucun élément permettant d'étayer cette hypothèse.

7. CONCLUSIONS

Aucun indice n'a été relevé permettant d'affirmer que le réseau Stay-Behind a été réinstauré ni sous la direction du SGR ni sous une autre forme.

SECTION 5 : LES CELLULES PROVINCIALES DU SGR ET LEURS ACTIVITES A L'EGARD DES CIVILS

1. INTRODUCTION

Le 24 avril 1996 est paru dans le journal «De Morgen» un article dont le titre est le suivant :

«L'ARMEE ESPIONNE LES CIVILS A GRANDE ECHELLE.

(...) Contrairement à tous les accords, le service d'espionnage de l'armée s'intéresse à nouveau fortement aux écologistes et militants en faveur de la paix, aux minorités de toutes sortes (comme les Basques et les Kurdes) et aux membres de sectes et personnalités issues du monde de la criminalité dans notre pays.

Notre rédaction dispose de preuves selon lesquelles le Service Général de Renseignement et de la Sécurité (SGR), sous la direction du Général (...), a mis au point un réseau d'informateurs sur l'ensemble du territoire pour infiltrer principalement la société civile. A cette fin, depuis l'automne de l'année passée, de nouvelles sections du SGR ont été créées ou les sections existantes ont été renforcées dans la quasi-totalité des chefs-lieux provinciaux.

(...) L'armée a affecté plus de vingt militaires professionnels pour infiltrer la société civile depuis des bâtiments militaires dans les chefs-lieux provinciaux.

Les informations des informateurs rémunérés seront ensuite traitées sous forme de rapports à l'attention du Service Analyse du SGR à l'Etat-major de l'Armée à Evere. Notre rédaction a pu localiser un certain nombre de cellules d'espionnage... à Hasselt (où est également établi le Commandement Militaire Provincial), ... à Gand, ... à Anvers (il s'agit dans ce cas des bâtiments militaires à la Marialei), ... à Liège (la Caserne Fonck).

En outre, il existe également des cellules de la Sécurité Militaire qui sont établies à Bruges, Namur et Charleroi.»⁽¹⁾

Cet article a provoqué de l'émoi dans le monde politique.

Le lendemain, d'autres journaux ont repris cette information, ainsi que les commentaires de parlementaires à ce sujet.

Ainsi, « Het Nieuwsblad » annonçait dans son édition du 25 avril 1996 :

« La fraction SP à la Chambre fait déjà grand cas de l'information. Selon Robert Delathouwer et Ronny Cuyt, l'espionnage des civils par l'Armée va à l'encontre de l'avis de la majorité du Parlement.»⁽²⁾

« Het Volk » titrait également le 25 avril 1996 :

«Le haut commandement de l'armée refuse de faire tout commentaire à propos de l'information communiquée dans «De Morgen » selon laquelle le Service de Renseignement Militaire se réorganise pour pouvoir espionner les civils.

⁽¹⁾ Traduction libre

⁽²⁾ idem

(...) La fraction SP à la Chambre exige que toute la clarté soit faite sur cette affaire.

(...) Le Ministre Poncelet, actuellement aux Etats-Unis, sera prié de fournir des explications. »⁽³⁾

De même, « De Financieel-Economische Tijd » consacrait une partie de ses colonnes à ce sujet :

« Le SP veut la lumière sur la Sécurité Militaire. »

Les journaux francophones se sont également penchés sur le sujet. Ainsi, « Le Soir » du 25 avril 1996 écrivait « *Le renseignement militaire en stratégie offensive. Le SGR intrigue gouvernement et Parlement.* »

Alors que « La Libre Belgique » annonçait :

« Les nouvelles attaques de la presse flamande contre le service général de renseignement et de la sécurité de l'armée ont créé la surprise chez le ministre de la Défense et son entourage.

(...) Je répondrai à la Chambre et au Sénat la semaine prochaine, nous a déclaré Jean-Pol Poncelet, informé du dépôt de demandes d'interpellation (...) relatives à l'existence d'un système de surveillance et de contrôle de certains civils par l'organe militaire. »

2. PROCEDURE

Au cours de la réunion du 25 avril 1996, le Comité R a décidé d'ouvrir d'office une enquête de contrôle ayant pour but de vérifier si les droits conférés aux particuliers par la constitution et la loi sont respectés par le SGR. Cette enquête a été ouverte suite à une lettre du ministre de l'Intérieur, qui renvoyait à l'article susmentionné, paru dans le journal «De Morgen» du 24 avril 1996.

Conformément à l'article 43 § 1 de la loi 18 juillet 1991, le Chef du Service d'enquêtes a averti le ministre de la Défense nationale le 25 avril 1996 qu'une enquête de contrôle avait été ouverte.

Par lettre du 26 avril 1996, les Présidents de la Chambre et du Sénat ont été informés, conformément à l'article 46 § 3 du Règlement d'ordre intérieur, qu'une enquête de contrôle avait été ouverte.

Dès le 3 mai 1996, divers journaux (comme «Het Laatste Nieuws», «De Morgen», «De Standaard», ainsi que «La Dernière Heure» et «Le Soir») ont annoncé que le ministre de la Défense nationale chargerait le Comité R d'une enquête sur la réorganisation et le fonctionnement des Cellules Provinciales du SGR, afin de dissiper tout doute.

Par lettre du 13 mai 1996, le ministre de la Défense nationale a communiqué au Comité R qu'il avait déclaré à la Chambre des Représentants vouloir charger le Comité R d'une enquête en rapport avec la réorganisation et les activités des Cellules Provinciales.

Le ministre a également demandé d'élargir le champ de l'enquête sur la motivation de la réorganisation et sur la légalité des activités des Cellules Provinciales.

Le 16 juillet 1996, le Comité R a procédé, en présence du Chef du Service d'enquêtes, à l'audition

⁽³⁾ idem

du Chef du SGR.

Le 18 juillet 1996, une apostille a été adressée au Chef du Service d'enquêtes le priant de procéder à l'audition approfondie du responsable de la Section SGR/CI, dont relèvent les Cellules Provinciales.

Un questionnaire détaillé a été repris dans l'apostille. En outre, le Comité R a prié le chef du Service d'enquêtes de bien vouloir visiter diverses Cellules Provinciales.

Des membres du Comité R seraient présents lors de ces visites. Le Comité R pouvait ainsi consulter les dossiers et fichiers sur place.

3. FONDEMENT DE L'ENQUÊTE

Les différents articles de presse ont donné lieu à une certaine agitation dans le monde politique, à la suite de laquelle le Comité R a ouvert une enquête d'office.

Certains parlementaires ont prié la Commission Parlementaire d'accompagnement des Comités Permanents de contrôle des services de police et de renseignement de charger le Comité R d'une enquête.

Le ministre de la Défense nationale a également demandé l'ouverture d'une enquête de contrôle.

Le ministre de la Défense nationale a répondu devant la Chambre aux interpellations conjointes de Monsieur Deleuze sur «Les activités du Service Général de Renseignement et de Sécurité » (n° 455) et de Monsieur Delathouwer sur «L'espionnage civil à l'intérieur du pays par le Service de Renseignement Militaire» (n° 458) (Chambre des Représentants - 2 mai 1996) en ces termes:

«L'information révélée dans le journal «De Morgen» du 24 avril 1996 concernant le «déploiement d'un réseau d'informateurs dans tout le pays afin d'infiltrer la société civile», doit être précisée comme suit : la décision de localiser des éléments du SGR dans les installations militaires des différentes provinces a été prise en 1993 par l'un des prédécesseurs du chef actuel du service. Ces sections sont désormais localisées dans les états-majors provinciaux existants. C'est cette décision qui est mise en oeuvre depuis l'année dernière, avec comme seul objectif de rationaliser les déplacements et les communications.

(...) Grâce à la décentralisation et à l'intégration dans une institution militaire existante, des déplacements inutiles vers et à partir d'Evere peuvent être évités, et les membres du personnel peuvent utiliser le réseau téléphonique militaire.

(...) Les missions et compétences du personnel de ces sections n'ont absolument pas été modifiées. Seuls deux membres du personnel supplémentaires ont été nommés à cette fin. Il n'est donc certainement pas question d'un développement de ce qui existait déjà auparavant.

(...) A la question de savoir si les activités des Sections Provinciales du SGR restent dans le cadre légal, je puis vous dire que le Comité R, chargé du contrôle, n'a encore formulé aucune critique à ce jour. Je n'ai donc aucune raison de douter de la légalité de ces activités.

(...) Pour écarter toutefois le moindre doute, j'ai l'intention de charger le Comité R d'une enquête sur la réorganisation et le fonctionnement des Sections Provinciales du SGR, et ce uniquement pour dissiper la méfiance de certains parlementaires à l'égard du SGR et son chef, et pour illustrer mon

attachement à un contrôle discret et efficace des services de renseignement.

(...) Reste la question de savoir si les Sections Provinciales du SGR entrent dans le domaine de la Sûreté de l'Etat...? Pour cette raison, une proposition de loi est en préparation, laquelle offre une base légale solide aux deux services et décrit dans le même temps leurs missions. Je souligne qu'il ne s'agit que d'une proposition de loi qui n'a pas encore de valeur obligatoire. Pour faire la lumière sur la situation actuelle et optimiser dès à présent la coopération entre la Sûreté de l'Etat et le SGR, les deux ministres responsables ont décidé de préparer un accord de protocole qui doit réglementer cette coopération. »

A la question n° 32 de Monsieur B. Anciaux datant du 2 mai 1996 concernant «L'espionnage des civils à grande échelle par l'armée» (Questions-Réponses - Sénat - 25 juin 1996), le ministre de la Défense nationale a donné une réponse similaire à celle mentionnée ci-dessus.

4. MISE EN PLACE DES CELLULES PROVINCIALES SGR/S (SECTION CI)

4.1. Bref historique

Il résulte de diverses déclarations qu'il existait déjà avant les années 70, des cellules provinciales qui dépendaient du SGR/S.

Leurs agents venaient chercher leurs missions sporadiquement au siège principal à Bruxelles, pour les remplir ensuite dans les provinces. Ils communiquaient les résultats de leurs missions au siège principal. Pendant cette période, leur lieu de travail n'était toutefois pas situé dans une caserne ou dans un bâtiment militaire.

Au cours des années 70, ce type de cellules a disparu. On a opté pour une recentralisation des activités.

Durant cette période, les agents qui habitaient en province, venaient chercher leurs missions quotidiennement au siège central à Bruxelles pour les exécuter en province.

Cette procédure entraînait des frais inutiles à charge du ministère de la Défense nationale. En outre, les membres des services extérieurs du SGR perdaient énormément de temps en de nombreux déplacements.

4.2. Décision visant à la création des détachements provinciaux SGR/S (Section CI)

Le 17 juillet 1996, le Comité R a reçu une copie du dossier «Postes provinciaux ».

Il en ressort que l'ancien chef du SGR a annoncé le 19 novembre 1993 la création des Détachements Provinciaux SGR/S, et ce, dans le cadre de la nouvelle organisation du SGR/S. Pour ce faire, l'infrastructure nécessaire devait être prévue dans certains quartiers militaires.

Ces détachements provinciaux constituent des subdivisions de la section SGR/CI (Contre-Ingérence).

4.3. Motifs de la décentralisation

Cette décentralisation permet d'optimiser l'intégration des inspecteurs dans leur secteur, en les basant à proximité des instances et organismes militaires et civils, avec lesquels ils doivent entretenir des contacts en rapport avec leur missions.

En outre, la disponibilité du personnel se voyait ainsi renforcée de manière considérable, grâce à la suppression des déplacements.

4.4. Situation après la décentralisation

A partir du 1^{er} mars 1995 ces Cellules Provinciales ont été mises en place progressivement. Elles ont été opérationnelles à partir de septembre/octobre 1995.

Il y a une section du SGR/S dans chaque province sauf celle du Luxembourg, assurée par la section de Namur. Il existe une section pour les provinces du Brabant flamand et wallon.

5. MISSIONS ET METHODES DE TRAVAIL DES CELLULES PROVINCIALES

Les Cellules Provinciales sont des subdivisions de la section CI.

La mission générale de la section SGR/CI consiste à mener des activités, dont le but est de découvrir, d'identifier et de combattre la menace qui provient de services de renseignement, d'organisations ou de personnes isolées hostiles et qui sont actives dans le domaine de l'espionnage, du sabotage, du terrorisme ou de la subversion, pour autant que leurs activités soient en rapport avec le domaine militaire (comme des actions dirigées contre les objectifs militaires, l'OTAN et l'armée en général), ainsi que les cas où le personnel de la Défense nationale (militaire ou civil) est concerné.

Les missions des services extérieurs sont divisées en missions permanentes et ponctuelles

5.1. Missions permanentes

Celles-ci sont exécutées par le biais de recherches dans le secteur ciblé, en tenant compte de la mission générale du SGR/CI et en fonction des directives qui lui sont transmises par le Chef du SGR/CI. Ces informations font l'objet de rapports officiels.

5.2. Missions ponctuelles

Il s'agit de missions écrites, émanant du Chef du SGR/CI ou des Cellules contre-espionnage, subversion ou terrorisme.

Ces dernières missions sont transmises par l'intermédiaire du Commissaire principal et du Chef du CI. Elles sont éventuellement complétées par les commentaires et directives du Commissaire principal en ce qui concerne leur exécution.

L'agent dispose d'une liberté d'action illimitée dans l'exécution de sa mission. Il doit toutefois respecter les directives et la loi.

Toutes les enquêtes sont effectuées le plus rapidement possible, en tenant compte du degré d'urgence.

Le siège principal envoie ces missions par écrit, en requérant la collecte des éléments essentiels d'information (EEI).

Les missions accomplies font l'objet d'un rapport qui est transmis au Commissaire en chef. Ce dernier complète ce rapport par des commentaires et propositions éventuels, avant de remettre ce document par l'intermédiaire du Chef du SGR/CI à la partie qui en a fait la demande.

6. MOYENS DES CELLULES PROVINCIALES

Selon l'infrastructure au sein du quartier militaire, les Cellules Provinciales peuvent disposer d'un ou de plusieurs locaux. Ces locaux sont équipés d'un minimum de mobilier et de moyens de communication, qui doivent permettre l'accomplissement des tâches administratives.

Les agents des services Provinciaux disposent de cartes de visite au nom du service avec le logo officiel.

7. LIEUX VISITES PAR LE COMITE R

Comme il a déjà été dit précédemment, des membres du Comité R, accompagnés de membres du Service d'enquêtes, ont visité 3 Cellules Provinciales.

Sur place, l'infrastructure, le personnel et les moyens dont disposent les services ont été examinés.

De plus, les missions exécutées par les services ont été contrôlées (entre autres à l'aide des registres et dossiers tenus à jour), le Comité R a pu constater que ces mentions correspondaient avec les explications fournies par le responsable du poste.

Aucun matériel d'écoute n'a été trouvé lors de l'enquête.

8. CONTRÔLE PAR LE SERVICE D'ENQUÊTES AU SIEGE PRINCIPAL DU SGR/CI

Le 8 novembre 1996, le Service d'enquêtes s'est rendu au siège du SGR/CI, afin de procéder au contrôle de la correspondance d'entrée et de sortie entre le siège principal et les sièges provinciaux.

Ils ont pris connaissance du registre IN-OUT (services externes).

Le Service d'enquêtes s'est fait présenter 54 documents choisis au hasard dans le registre, en prenant soin ainsi d'examiner le travail de toutes les cellules provinciales.

Il a été établi de manière détaillée, grâce à l'examen des documents consultés, que les informations réunies ont un rapport avec la consultation de sources ouvertes, et qu'elles concernent effectivement la problématique de la sécurité de l'armée. Elles relèvent en conséquence de la compétence du SGR.

9. CONCLUSIONS

Il ressort de l'enquête menée par le Comité R que :

1. Dans le passé, il existait déjà, dans les provinces, des cellules qui constituaient des

subdivisions du SGR. Ces cellules ont progressivement disparu dans les années 70.

2. La décision de créer des cellules provinciales du SGR date du 19 novembre 1993. Ces cellules ont été créées dans le but d'éviter une perte de temps pour les agents et de réduire les frais.

3. Les cellules provinciales agissent sous la responsabilité du SGR/CI et ont pour mission de :

« Mener des activités, dont le but est de découvrir, d'identifier et de combattre la menace qui provient de services de renseignement, d'organisations ou de personnes isolées hostiles qui sont actives dans le domaine de l'espionnage, du sabotage, du terrorisme ou de la subversion, pour autant que leurs activités soient en rapport avec le domaine militaire (comme des actions dirigées contre les objectifs militaires, l'OTAN et l'armée en général), ainsi que les cas où le personnel de la Défense nationale (militaire ou civil) est concerné. »

Elles effectuent des missions permanentes et ponctuelles.

4. Le travail au sein de ces cellules provinciales se déroule conformément aux directives données par le siège principal. Ce travail est contrôlé par le siège principal.

5. Les agents des cellules provinciales, une fois opérationnels, ont pris immédiatement contact avec les autorités locales. Il n'est certainement pas question d'activités secrètes.

6. Le Comité R n'a relevé aucun indice permettant d'établir que les droits, que la Constitution et la loi confèrent aux personnes, ont été violés par le travail de renseignements, accompli par les cellules provinciales sous la responsabilité du SGR/CI.

CHAPITRE 2 : ENQUÊTE SUR LA CRÉATION ÉVENTUELLE D'UN NOUVEAU SERVICE DE RENSEIGNEMENT MILITAIRE

1. INTRODUCTION

Un article sous le titre "L'armée craint une menace immigrée" paru dans le journal "le Soir" du 30 juillet 1996 sous la plume du journaliste Alain Guillaume a provoqué des remous dans les milieux politiques.

D'après cet article, une section des forces Armées belges CTI (Commandement Territorial Interforces) avait établi un document à caractère xénophobe. Ce document a pour intitulé "Concept pour la défense militaire du territoire" et émane du commandement territorial interforces.

L'article reprend des passages de l'analyse de la menace actuelle : *" De nombreuses communautés d'immigrés se sont fixées dans les grandes agglomérations. Si ces groupes de population devaient entrer clairement en désaccord avec la politique belge, ils pourraient déclencher des actions visant à contrarier cette politique ou visant à faire connaître leurs mécontentements (...). Nous considérons qu'il n'existe aucune menace ouverte en Belgique (...). Mais il existe bien une menace clandestine avec un caractère permanent".*

Cet article établit un lien direct entre la mission de collecte de renseignements de la Défense Militaire du Territoire, le SGR et le réseau "Stay behind". On lit en effet : *"S'il n'est étroitement lié aux activités du Service général de renseignement (ce qui serait étonnant) ce réseau n'est donc rien d'autre qu'une nouvelle structure de renseignement militaire curieuse des soubresauts de la société civile et particulièrement méfiante à l'égard de ce qui lui est étranger".* Plus loin, sous le sous-titre *"La Moslavie menaçait la Belgique"*, on lit : *"Un plan important des plans de défense s'écroulait avec la disparition des "Stay behind" (...). Il était évident que d'une manière ou de l'autre, "quelque chose" devrait remplacer les "Stay behind", au moins partiellement. Ce "quelque chose" est donc constitué des unités de défense du territoire du commandement territorial interforces".*

2. PROCÉDURE

Au cours de sa réunion du 7 août 1996, le Comité R a décidé d'ouvrir d'initiative une enquête fondée sur l'article 3- 2° de la loi organique du 18 juillet 1991, qui prévoit la compétence du Comité R *"... sur tout service public spécialement chargé, après l'entrée en vigueur de cette loi, de la collecte et du traitement de données concernant des personnes, groupes et événements et effectuées dans un but de sécurité".*

Cette enquête a pour but de vérifier si, comme l'affirme la presse, un nouveau service de renseignement militaire a été créé, quels en sont notamment les missions, les méthodes et les moyens. Le Comité R a également pour objectif d'enquêter sur l'implication éventuelle du SGR dans l'élaboration du document paru dans la presse et rédigé par le colonel De Vleeschouwer en 1995.

Par lettre du 8 août 1996, les présidents du Sénat et de la Chambre, ont été, conformément à l'article 46 alinéa 3 du règlement d'ordre intérieur, informés de l'ouverture de l'enquête.

Le chef du Service d'enquêtes a adressé le 20 août 1996 une lettre au ministre de la Défense nationale portant à sa connaissance l'ouverture de cette enquête conformément à l'article 43 alinéa 1 de la loi organique du 18 juillet 1991.

Le Comité R assisté de son Service d'enquêtes a procédé dans le courant des mois d'août et septembre 1996 à l'audition du responsable du SGR, du chef des forces Armées belges, du général Brunin et du colonel De Vleeschouwer (responsables de la section CTI au sein des forces armées belges).

Par diverses apostilles du mois d'août, septembre et octobre 1996 le Comité R a chargé le Service d'enquêtes de procéder à plusieurs devoirs dont notamment celui de prendre connaissance des dossiers établis par les Forces de l'intérieur et par le CTI ensuite, constituant toutes deux consécutivement des sections des forces Armées belges.

3. MOTIF DE L'ENQUÊTE

Une partie du monde politique et social a été choqué par le contenu du document incriminé. La presse s'est fait l'écho de nombreuses déclarations défavorables.

Le ministre de la Défense nationale a déploré dans un communiqué de presse à l'agence Belga que :

- "une fois de plus des documents classifiés aient été rendus publics";
- "le document litigieux *"n'est qu'un projet émanant de l'ITC"*;
- "ainsi que l'indique sa page de garde qui mentionne ses destinataires, ce document n'a été soumis ni aux chefs d'états major, ni au ministre de la Défense nationale";
- "*le document en question n'exprime ni le point de vue de l'armée ni celui du ministre"*;
- "*il regrette vivement que le document en cause donne une présentation simpliste, réductrice, voire même choquante de la réalité. En fait, en cas de conflit, la menace pourrait émaner de tout groupe ou individu dont la loyauté à l'égard de l'Etat belge est suspecte. Ce manque de loyauté pourrait être dû soit au fait que ces groupes ou individus sont acquis à un état étranger, soit au fait qu'ils contestent la forme démocratique de l'Etat ou l'existence même de celui-ci"*;
- "*la lecture du document pourrait donner l'impression que l'on confie à des réservistes des tâches de collecte de renseignements en temps de paix, ce qui serait évidemment anormal, même si c'était en vue de faire face aux exigences en temps de guerre."*
- Le ministre de la Défense nationale veillera "*à ce que cette ambiguïté soit levée. Il ne saurait en aucun cas être question d'établir des réseaux de renseignements parallèles. En effet, eu égard à la nécessité de protéger la vie privée, il est impensable de confier la collecte de renseignements militaires à des non professionnels en dehors d'un cadre légal et de mécanismes de contrôle efficaces."*

Certains membres de partis politiques ont également fait des déclarations à la presse. Les

passages les plus marquants sont les suivants :

- Mostapha Ouezekhti, député Ecolo au Conseil régional bruxellois a déclaré que : *“ il s’agit d’un drame dérapage dans les relations que nous devons entretenir avec les populations d’origine étrangères installées légalement, et souvent depuis très longtemps, en Belgique. (...)”*

Je me demande si les responsables militaires à l’origine de cette funeste note ont songé un seul instant à l’impact que leur analyse pouvait avoir sur ceux qui sont désignés comme les nouveaux ennemis.” (Le Soir du 1^{er} août 1996).

- Michel de Herde, échevin PRL-FDF à Schaerbeek a aussi fait des déclarations à la presse. *“En désignant les immigrés comme une menace clandestine avec un caractère permanent, les responsables militaires de cette structure accréditent officiellement une thèse de l’extrême droite qui désigne des dizaines de milliers de citoyens comme des terroristes en puissance. Dès lors, afin que cesse cette mascarade d’espions paranoïaques, je demande dès aujourd’hui aux parlementaires démocrates, en particulier à ceux de mon parti, d’interpeller le ministre de la Défense afin qu’il dissolve ce réseau militaire.”* (Le Soir du 1^{er} août 1996)

D’autres réactions sont favorables au document litigieux. Le Comité R les mentionne par souci d’objectivité.

Ainsi le journal “Pallietkerke” a pris fait et cause pour les services de renseignement militaires dans un article publié le 7 août 1996. En substance, ce journal estime qu’à bon droit les services de renseignement militaires rassemblent des informations sur les immigrés.

Le journal “Gazet van Antwerpen” mentionne dans un article paru le 9 août 1996 que le patron de l’OTAN, Willy Claes, a désigné le monde arabe comme ennemi potentiel.

Enfin la presse internationale a tendance à accroître les rumeurs sur base de quelques informations dont elle dispose en manière telle que l’agence France presse a diffusé sur une base de données informatisées disponible pour la presse internationale un message le 30 juillet 1996. Ce communiqué laisse entendre qu’en Belgique le renseignement militaire belge a créé une unité spéciale qui a pour mission de suivre les communautés d’immigrés en Belgique.

Le Comité R a également pris connaissance d’un certain nombre de questions et d’interpellations parlementaires.

- ? question n° 48 du 1^{er} août 1996 au Sénat de M. Fred Erdman chef du groupe SP du Sénat au ministre de la Défense nationale.

Cette question concerne aussi les suites de la commission d’enquête Gladio. Elle tend à permettre à la commission sénatoriale compétente de procéder à une enquête, à ce propos.

Le ministre a répondu le 9 septembre 1996 que tout sera mis en oeuvre pour empêcher que les forces armées puissent apparaître à cause du comportement ou de maladresses de certains comme cautionnant les discours racistes de l’extrême droite.

- ? question n°53 au Sénat de M. Destexhe du 30 août 1996 au ministre de la Défense nationale: Commandement Territorial Interforce;

Une des caractéristiques du plan de restructuration de l’armée belge a été la création d’un Commandement Territorial Interforce (CTI).

Ce concept a suscité quelques crispations.

1. Depuis quand le CTI est-il opérationnel ?
2. Pouvez-vous évaluer le fonctionnement de ce nouvel outil, ce nouveau concept ?
Êtes-vous satisfait ? Envisagez-vous une évolution ou des modifications dans le fonctionnement de ce CTI ?

Réponse : l'honorable membre est prié de trouver ci-après la réponse à ses questions.

1. Le Commandement Territorial Interforces (CTI) est opérationnel depuis le 1er juillet 1995.
2. Pour ce qui est des compétences et de la structure du CTI en particulier la dépendance fonctionnelle du Groupement d'appui médical, des décisions seront prises prochainement. Quoiqu'il en soit, les principes de mise en commun des moyens, de personnel et d'infrastructure entre les diverses composantes des forces armées ne seront pas remis en question. En suivant cette ligne, on peut réunir des équipements, regrouper des commandes et partager certains services. Cette politique de "single management" sera poursuivie. Il est clair toutefois que des leçons seront tirées de la mise en place et des premiers mois de fonctionnement du CTI, afin d'en faire un outil efficace et efficient.

? question à la Chambre des Représentants du 19 septembre 1996, n° 617 de M. Olivier Deleuze (Ecolo) au ministre de la Défense nationale sur "le plan de base de la défense militaire du territoire".

? question à la Chambre des Représentants du 19 septembre 1996, n° 618 de M. Lode Vanoost (Agalev) au ministre de la Défense nationale sur "le plan militaire de défense nationale".

Ces questions publiées dans le compte rendu analytique de séance plénière n° 98 ont été renvoyées à la commission de la Défense nationale.

La crédibilité du SGR est donc mise en cause.

4. APPROCHE DES DIFFÉRENTES NOTIONS MENTIONNÉES DANS LE MONDE DU RENSEIGNEMENT

Dans la présente enquête, il sera à plusieurs reprises question des notions suivantes :

1. le renseignement stratégique;
2. le renseignement opérationnel;
3. le renseignement tactique;
4. le temps de guerre;

Dans un premier temps il convient de rappeler la définition du renseignement tel que le Comité R l'a fait dans son rapport précédent ⁽¹⁾ :

Le renseignement est un ensemble des connaissances de tous ordres sur un adversaire potentiel, utiles aux pouvoirs publics et au commandement militaire. En d'autres termes le renseignement est une information traitée, analysée et diffusée à qui de droit.

Les différents types de renseignements dont il est question dans le présent rapport concernent davantage les forces armées belges que le service civil de renseignement représenté par la Sûreté

⁽¹⁾ Rapport d'activités du Comité R. - 1996 - p.21

de l'Etat. C'est la raison pour laquelle le Comité R a demandé au SGR de lui faire parvenir sa conception de ces notions, en se basant pour ce faire sur les approches de ces concepts faites par l'OTAN.

Le responsable du SGR définit ces notions (que le Comité R fait siennes) de la façon suivante :

1. "Renseignement stratégique"

Il s'agit, d'une part, du renseignement nécessaire à la prise de décision au plan national (gouvernement) ou international (ONU, OTAN, UEO), et, d'autre part, du renseignement utile en matière de planification par l'autorité militaire (Etat-major général ou supérieur) d'une opération en appui de cette décision.

Il y a donc lieu de collecter des informations relatives à une puissance ou un groupe de puissances dans les domaines suivants : biographie, économie, sociologie, transports et télécommunications, géographie militaire, forces armées, politique, science et technologie.

Exemple

Dans le cadre des accords de DAYTON, la décision prise par l'OTAN de déployer la force multinationale IFOR, la préparation de la décision du gouvernement belge et la planification par l'Etat-major général de la mise en oeuvre de la composante belge pour les opérations en ex Yougoslavie ont nécessité ce type de renseignement.

2. Renseignement opérationnel

Il s'agit du renseignement nécessaire pour la planification et la conduite de campagnes et d'opérations importantes visant à atteindre des objectifs stratégiques dans des théâtres ou des zones opérationnels.

Il englobe le renseignement sur les moyens militaires, la structure des forces, la doctrine, l'armement, les équipements, les infrastructures, l'instruction et les intentions des pays ennemis ou des parties en présence en cas d'opérations de paix.

Exemple

Ce type de renseignement permet au commandant du théâtre des opérations en Bosnie-Herzégovine (le commandant de l'IFOR) de planifier et de mener à bien cette opération de maintien de la paix et donc, d'atteindre ses objectifs stratégiques, en l'occurrence, l'établissement des conditions sécuritaires nécessaires à la résolution politique du conflit.

3. Renseignement tactique

Il s'agit du renseignement qui permet au commandant tactique de préparer et de mener à bien des opérations tactiques à son niveau (bataillon, brigade, division, éventuellement corps d'armée). Il comprend la connaissance de l'ennemi ou des parties en présence (en cas d'opérations de paix), des circonstances géographiques et atmosphériques (météo) et de l'attitude de la population civile dans et autour de la zone d'action considérée.

Outre la connaissance de la doctrine et des procédés tactiques, de l'effectif, de l'armement et du matériel de l'ennemi ou des parties en présence (forces armées et organismes paramilitaires), le commandant tactique a besoin de renseignements relatifs au terrain dans lequel vont se déployer

ses troupes.

Exemple

C'est de ce type de renseignement dont a besoin le commandant du bataillon Belbat, déployé dans le cadre de l'ATNUSO (Administration Transitoire des Nations Unies en Slavonie Orientale) afin de mettre en oeuvre son unité dans sa zone d'action (la Baranja)."

Le Comité R propose des définitions vues d'un autre point de vue : celui du résultat alors que le SGR donne une approche qui concerne plus le contenu

1. Le renseignement stratégique militaire

Action de coordonner la récolte, le traitement et l'analyse des informations dans le contexte politique, économique, social et militaire d'un ou de plusieurs pays.

2. Le renseignement opérationnel militaire

Action de récolter, de traiter et d'analyser des informations relatives à des opérations militaires.

3. Le renseignement tactique militaire

Action de récolter, de traiter, et d'analyser des informations dans le but d'exercer l'art de diriger une bataille, en combinant par la manoeuvre l'action des différents moyens de combat et les effets des armes.

4. Le temps de guerre

Le temps de guerre est défini par l'article 58 de la loi du 15 juin 1899 titre II.

Il s'agit d'une situation exceptionnelle qui entre en vigueur par arrêté royal décidant de la mobilisation générale et prend fin par arrêté royal décidant de mettre les forces armées sur pied de paix.

5. SYNTHÈSE DE L'ENQUÊTE

5.1. Position du problème

La clarté de l'exposé de cette enquête impose dans un premier temps de situer le Commandement Territorial interforces (CTI) dans l'organigramme des forces armées belges.

Les forces armées belges ont fait l'objet d'une réorganisation en 1989. Cette décision du ministre Delcroix, ministre de la Défense nationale à l'époque, a été transcrite dans l'arrêté royal du 19 décembre 1989 portant organisation de l'état-major général et dans l'arrêté royal du 13 juin 1995 sur le Commandement Territorial Interforces (CTI).

Le CTI est une des quatre sections des forces armées belges, les trois autres étant les forces terrestre, aérienne et la force navale.

L'arrêté royal du 13 juin 1995 mentionne que le CTI relève directement de l'autorité du chef d'Etat-major général.

L'article 15bis § 2 de cet arrêté royal précise les attributions de cette section des forces armées :

“1° assurer des missions dans le cadre de l'assistance au profit de la nation;

2° assurer la planification et la coordination de missions relatives à la sécurité du territoire national, le déminage et la mise en oeuvre de moyens de génie, de moyens de transmissions ainsi que de moyens médicaux;

3° assurer des missions d'appui au profit des forces armées;

4° assurer l'appui aux autorités et unités militaires alliées sur le territoire national.”

Ces attributions sont pratiquement les mêmes que celles des Forces de l'Intérieur, section des forces armées belges, supprimée par le plan Delcroix ci-dessus mentionné.

Une des missions du CTI consiste à protéger militairement le territoire national (cf. 2° de l'art. 15bis §2, 2° de l'arrêté royal du 13 juin 1995). Cette mission est intitulée Défense Militaire du Territoire (DMT).

Le général en chef de la force terrestre est le responsable de l'organisation de la Défense Militaire du Territoire (moyens, matériel, formation) tandis que le chef d'Etat-major des forces armées est le responsable de la mise en oeuvre.

Les cadres des réservistes (officiers et sous-officiers) effectuent des exercices de défense de points et d'installations sensibles sur le territoire national. L'ensemble des réservistes (cadre + troupe) est au nombre de 8.600 hommes environ. Ils sont regroupés en unité provinciale, soit 1.000 hommes par province à peu près. Ces exercices sont organisés pour familiariser les réservistes aux missions qui leur seront imparties en temps de guerre.

Le colonel De Vleeschouwer est le responsable de la bonne fin de ces exercices sous l'autorité du général Brunin.

5.2. Le “concept” de la défense militaire du territoire

Afin de pouvoir remplir la tâche impartie, il faut disposer, d'après le commandement du CTI, d'un concept qui définisse ou qui donne à tout le moins une évaluation des menaces potentielles. Il faut également préciser la façon dont les points vitaux doivent être défendus, les moyens dont il faut disposer et la manière dont il faut mettre au courant les unités chargées de la mission.

Pour ce faire le chef d'Etat-major demande au chef du SGR d'établir une note, document interne à l'état-major, qui décrit l'environnement, c'est-à-dire l'approche de la menace actuelle, dans lequel le concept de Défense Militaire du Territoire doit être élaboré.

La note sur laquelle s'est basé le colonel De Vleeschouwer pour établir le document controversé date du 7 avril 1993.

Les risques de sécurité interne au territoire national sont divisés en cinq chapitres :

- généralités;

- espionnage;
- subversion;
- terrorisme;
- risques nouveaux.

Ce dernier chapitre, rédigé en néerlandais, peut être traduit de la manière suivante :

“Le monde actuel se caractérise par sa complexité et son instabilité, où de nouveaux risques voient le jour et où d’autres risques deviennent de plus en plus importants.

(1) Le fanatisme religieux (entre autres le fondamentalisme islamiste) qui se développe dans le flanc sud de l’Europe et qui, déjà, crée des problèmes graves dans des pays tels que l’Algérie et l’Égypte, constitue un risque important avec lequel les pays de l’Ouest seront confrontés dans le futur. La présence de minorités étrangères en Europe occidentale ne peut qu’aiguiser le problème.

(2) Les migrations

Les perspectives futures pour une grande partie des pays africains et pour certains pays asiatiques sont peu porteuses d’espoir. L’augmentation de la population dépasse la croissance économique, ce qui génère et propage rapidement la famine et des maladies infectieuses (ou contagieuses). Cela a pour conséquence le déplacement du flux de l’immigration du sud vers le nord et vers les pays riches de l’ouest. Les développements politiques récents en Europe ont également créé un courant de réfugiés de l’Est vers l’Ouest. La disparition du rideau de fer et l’ouverture des frontières européennes ont facilité les migrations.”

5.3. Analyse du document paru partiellement dans la presse

Le Comité R a pris connaissance du texte intégral de ce document controversé.

C’est sur base du document repris dans le sous chapitre précédent que le colonel De Vleeschouwer a rédigé le texte qui a provoqué les réactions décrites ci-dessus.

Ce texte est intitulé “Concept DMT” et est daté du 16 août 1995. Il est classifié “confidentiel”. Il est diffusé à l’intérieur des forces armées belges et 66 photocopies ont été adressées notamment au chef de l’état-major section opération, aux commandements provinciaux et aux différents services de l’état-major du CTI. A chaque destinataire, il est demandé de faire part de ses remarques éventuelles. Ce document précise qu’il *“ est un projet et donc susceptible d’être amélioré. Cela doit permettre au Bn DMT de prendre en charge immédiatement son instruction et son training militaire et ainsi de motiver “les réservistes actifs”. Il est demandé aux destinataires de ce document de l’étudier en profondeur et de faire part de leurs propositions constructives dans un but d’amélioration.”*

Des remarques, propositions et surtout des questions ont été adressées au colonel Devleeschouwer conformément à sa demande. Ces remarques sont au nombre de 9. Une seule concerne la menace. Cette remarque est la suivante : *“il faut éviter de faire un procès d’intention aux communautés d’émigrés”*. Ce militaire était donc sensible au respect qu’il convient d’accorder aux communautés d’immigrés.

5.3.1. En ce qui concerne la définition de la mission

Le Comité R a relevé les passages suivants dans la Section 1 -Introduction de la note litigieuse CTI:

“Surveiller

Surveiller un point sensible consiste à recueillir des informations qui transmises à l’Ech Sup lui permettra de prendre des mesures.

Surveiller n’implique pas nécessairement une action de Comb ni une présence permanente.

Les éléments de surveillance mènent leurs actions :

- *par l’exécution de patrouilles mobiles à des intervalles irréguliers sur les points à surveiller et sur leurs environs*
- *à partir de postes fixes.”*

A la section 2 du document sont évoquées les hypothèses de départ :

1. la DMT dans le cadre d’un scénario de crise croissante;
2. le rappel du personnel a un caractère évolutif;
3. la contribution du Host Nation est limitée;
4. considérations d’ordre opérationnel;
5. considérations d’ordre tactique;
6. considérations d’ordre structurel;

PREMIER COMMENTAIRE

Le Comité R s’interroge sur la nécessité de définir une menace actuelle de manière aussi large et générale alors que la mission des réservistes se limite à protéger des “points sensibles”. Le rôle du CTI n’est pas de faire du renseignement stratégique.

Le Comité R estime qu’il suffit de faire la distinction entre la menace militaire et la menace émanant de groupes terroristes ou subversifs de n’importe quelle origine.

5.3.2. En ce qui concerne l’aspect xénophobe de la définition de la menace

La section 3 du document décrit la menace actuelle dans les termes suivants :

“1. Nous constatons qu’un grand nombre de pays et de nations désirent vivre suivant le modèle occidental. Pour preuve en sont les modifications en Europe de l’Est et les tensions de démocratisation entre autres en Afrique. Simultanément de plus en plus d’étrangers de différentes origines, surtout d’Afrique qui est un des plus important fournisseurs de matière première, viennent s’installer dans les pays de la Communauté Européenne.

2. De nombreuses communautés d’immigrés se sont fixées dans les agglomérations où l’on retrouve les principaux organes de direction, les ports et les centres industriels. En cas de désaccord de ces groupes de population avec la politique belge, ils sont à même de déclencher des actions visant à fléchir cette politique ou en faisant connaître leurs récriminations.”

3.a. Nous pouvons au su de l’absence d’interventions et d’actions actuelles, nous limiter à la perception des possibilités de chaque adversaire potentiel.

En conséquence, en tenant compte de ce qui précède, nous acceptons qu'il n'existe aucune menace ouverte en Belgique car cela exigerait de l'adversaire potentiel des préparatifs militaires avancés. Il existe toutefois une menace clandestine à caractère permanent.⁽²⁾ Un ennemi potentiel exécute dès le temps de paix une partie de ses missions, les intensifie en cas de crise et lors du conflit."

Aucune compétence judiciaire n'étant dévolue au Comité R, il ne s'autorise pas à se prononcer sur les éléments de l'infraction décrite dans la loi du 30 juillet 1981 sur le racisme et la xénophobie que pourrait contenir le document litigieux.

Le Comité R estime néanmoins qu'associer de manière ambiguë la présence de communautés d'immigrés sur le territoire national à une "menace clandestine à caractère permanent" constitue une atteinte à la dignité des nombreux ressortissants étrangers qui résident dans notre pays.

Une telle vision des choses ne s'inscrit certes pas dans la ligne du programme gouvernemental qui, en son chapitre II.A.3 prévoit que "la présence stable en Belgique de personnes d'origine étrangère doit être considérée comme un apport positif pour notre société." Le gouvernement rappelle "avec insistance qu'il poursuivra la lutte contre toute forme de racisme, d'antisémitisme et de xénophobie".

C'est en cela que la note controversée est critiquable.

5.3.3. En ce qui concerne la mission de renseignement du CTI

La section 7 de ce document traite de l'instruction et de l'entraînement. Ce dernier point est développé sur le plan opérationnel et sur le plan tactique.

Les procédés sont précisés en ce qui concerne la récolte de renseignements. Cette mission est décrite de la manière suivante :

(a) Procédés

Chaque membre du cadre doit être entraîné en tenant compte de la fonction qui lui est attribuée. Durant les rappels l'accent sera mis sur la connaissance des procédés suivants :

- (I) Surveillance, sûreté, défense et dégagement de points sensibles*
- (ii) Récolte et diffusion de renseignements*
- (iii) Surveillance de LOC (lire locaux)*
- (iv) Diffusion d'ordre à tous les Ech. (lire échelons)*

(b) Dossiers

- (i) Le comd de Bn (lire Commandant de Bataillon) établira un dossier pour chaque PS (lire point sensible) de sa prov chaque dossier comportera au minimum :
- emplacement et description du PS
- les ordres de surveillance - de sûreté - de protection et du dégagement éventuel du PS*
- (ii) Les plans de Pat pour la surveillance du PS seront établis en détail.*
- (iii) Les plans de surveillance des LOC qui passent dans la Prov (lire province) feront l'objet d'un seul dossier.*

⁽²⁾ Souligné par le Comité R

Remarque : Ces dossiers devront être prêts avant le 31 décembre 1996. Ils seront clairs et précis et suffisamment détaillés que pour permettre une utilisation par les Elm (lire éléments) de la Fint (lire force interne) chargés de missions DMT éventuelles en temps de crise en attendant que les Bn DMT (lire bataillon défense militaire du territoire) soient Ops. (lire opérationnels). Ces derniers sont conservés à l'EM Prov. (lire état major provincial).

Récolte de renseignements

La mission de la DMT se base sur la récolte de renseignements.⁽³⁾ Les unités oeuvreront dans la Prov (lire province) comme des agents de quartier.⁽⁴⁾ De ce fait une relation de confiance devra se créer entre le Pers (lire personnel) et la gendarmerie, les services de police, les gardes champêtres, les gardes forestiers de la Prov et aussi la population habitant aux alentours des PS (lire points sensibles)⁽⁵⁾. Ces contacts doivent être établis dès le temps de paix⁽⁶⁾, de préférence à l'occasion des rappels. Il est dès lors conseillé d'établir une liste⁽⁷⁾ avec les autorités et les services avec leur adresse, Tf (lire téléphone) et N° de fax ainsi que d'autres données jugées nécessaires.⁽⁸⁾

Le général Brunin a réagi à l'occasion d'une conférence de presse le 1^{er} août 1996. Ce communiqué, donné en néerlandais, dont il a été fait mention dans le journal "Het Volk" du 1^{er} août 1996, peut être traduit de la manière suivante :

"Nous voulons rassembler des renseignements sur nos ennemis potentiels pour protéger notre territoire et nos lignes de communications en temps de guerre et si nécessaire, les défendre. Nous voulons en conséquence nous renseigner sur les éléments et groupes potentiellement dangereux des différentes couches de la société, sur les civils belges et groupements, sur les groupes néerlandais, français allemands ou américains mais aussi sur les immigrés et les mouvements d'immigrés qui appartiennent aussi à notre société."

DEUXIÈME COMMENTAIRE

Le Comité R constate que :

? D'une part, les propos du général Brunin, tels que rapportés par le journal "Het Volk" le 1^{er} août 1996, comprennent les éléments de la définition de renseignement telle que donnée par le dictionnaire Larousse : "Ensemble des connaissances de tous ordres sur un adversaire potentiel, utiles aux pouvoirs publics et au commandement militaire".

? Ensuite la conception du document correspond au cycle du renseignement qui se décompose en quatre phases :

(3) Souligné par le Comité R

(4) Idem

(5) Idem

(6) Idem

(7) Idem

(8) Idem

- la direction de la recherche (cf. la menace potentielle);
- la recherche d'informations (cf. la récolte de renseignements);
- le traitement des informations (cf. l'établissement de dossiers);
- l'utilisation du renseignement (cf. la conservation des dossiers à l'état major provincial);

Ces phases ont été détaillées notamment dans le rapport d'enquête sur le Rwanda et sur la proposition des sources ouvertes faites par le Comité R dans son rapport d'activités 1996⁽⁹⁾.

? Enfin la définition de la menace potentielle faite par le document relève bien d'une analyse du renseignement stratégique en tant qu'elle désigne les communautés d'immigrés comme des ennemis potentiels. Cependant, cet essai de définition résulte de la seule initiative du rédacteur. Il s'agit d'une interprétation personnelle du rédacteur de l'analyse du renseignement stratégique faite par le SGR.

Il ne ressort cependant pas du document que les officiers de réserve aient reçu comme consigne spéciale de s'intéresser plus particulièrement aux communautés immigrées résidant dans les alentours des points sensibles.

? Les officiers sont certes chargés de surveiller des objectifs déterminés. Mais cette récolte des informations se passe d'une manière totalement différente des méthodes de travail du SGR. Ici, l'officier chargé de la surveillance d'un point sensible est encouragé à récolter lui-même les informations dont il a besoin pour sa propre mission. Ces informations doivent être directement opérationnelles; elles sont directement analysées et exploitées par l'officier sans passer par le cycle du renseignement exposé plus haut.

Le Comité R estime que l'analyse du document controversé et de la déclaration du général Brunin à la presse indique effectivement qu'une structure de réseau de renseignement militaire tactique a été couchée sur papier en temps de paix. Cette structure est indépendante du SGR.

5.4. Analyse des dossiers

Le Comité R a estimé que sur base de cette première analyse, il convenait de poursuivre l'enquête par l'étude des dossiers dont il ignorait l'existence dans la première phase de ses investigations.

Le 9 septembre 1996, le Comité R a prié le Service d'enquêtes de prendre connaissance et d'analyser les dossiers constitués par la section Forces Intérieures, dénommée CTI par la suite. Ces dossiers sont établis conformément à la note controversée.

Le Service d'enquêtes a rendu visite au colonel Pochet responsable de l'Etat-major général militaire de la région Bruxelles-Brabant.

De l'étude de ces documents et de l'entretien qu'il a eu avec le colonel Pochet, le Service d'enquêtes a relevé les éléments suivants :

Les dossiers "points sensibles" ont pour but de fournir des informations indispensables aux unités actives en cas de mobilisation. Ces dernières disposent ainsi de toutes les informations nécessaires afin d'assurer la protection des points sensibles en attendant l'arrivée des unités de

⁽⁹⁾ Rapport d'activités du Comité R 1996 p. 120 et suivantes et p.198

réserve dont la mission est de défendre ces points sensibles.

Dossiers de "points sensibles" établis jusqu'au 1^{er} janvier 1995 (par les Forces Intérieures) :

Le Service d'enquêtes n'a pas trouvé, dans les dossiers consultés, d'éléments qui renverraient vers des contacts non militaires situés dans les environs des points sensibles.

Dossiers de "points sensibles" établis après 1^{er} janvier 1995 par CTI

Au début du mois d'avril 1996 un modèle informatisé de dossier "points sensibles" a été envoyé à chaque Etat-major provincial. Des dossiers devaient être établis sur base de ce modèle et renvoyés avant la fin de l'année 1996 à la section G3 (Opérations) du CTI. Au 30 septembre 1996 la majorité des dossiers étaient rentrés.

Un dossier se compose de 11 chapitres :

1. Identification du point sensible
2. Situation
3. Pliage de la carte au 1/50.000
4. Description des installations permanentes
5. Personnes occupant le point sensible dès le PP (lire pied de paix)
6. Croquis des installations
7. Possibilités ennemies
8. Aide possible venant du civil
9. Forces affectées au PS
10. Attitude initiale sur le PS
11. Liste des annexes

Deux chapitres de ces dossiers ont spécialement attiré l'attention du Service d'enquêtes; il s'agit des chapitres relatifs aux personnes civiles ou militaires qui sont responsables des points sensibles ou qui peuvent y donner accès, d'une part, aux autorités civiles à contacter pour organiser la défense de ces points d'autre part.

Suite aux commentaires parus dans la presse fin juillet - début août 1996, le Colonel Marchal, chef d'Etat-major du CTI, a envoyé le 13 août 1996 aux postes de commandements provinciaux une rectification du concept de la Défense Militaire du Territoire. Dans cette rectification il est signalé que le passage concernant les communautés d'immigrés doit être modifié.

En outre il est recommandé d'éviter toute ambiguïté en reprenant uniquement les services officiels comme source d'information.

Les dossiers "Points sensibles" de la région militaire "Bruxelles-Brabant" ont été vérifiés par le colonel Pochet suite à la directive du colonel Marchal. Le colonel Pochet, puis ensuite le Service d'enquêtes du Comité, ont constaté que les dossiers ne contenaient aucune donnée relative à des civils.

Un nouveau modèle, adapté pour le chapitre 8, sera bientôt transmis par le colonel Devleeschouwer aux postes de commandements provinciaux.

TROISIÈME COMMENTAIRE

Tous les dossiers et documents demandés au colonel Pochet ont été remis au Service d'enquêtes sans réticence.

Le Service d'enquêtes du Comité R n'a pas trouvé d'élément dans ces dossiers qui indiquerait que des informations sont collectées sur des communautés d'immigrés.

Le Service d'enquêtes n'a retrouvé aucun élément dans ces dossiers qui indiquerait que des civils sont utilisés par l'armée en temps de paix comme informateur.

Les réservistes n'ont pas rempli le chapitre 8 des dossiers.

6. EVOLUTION

6.1. La défense militaire du territoire

Le 23 août 1996, le SGR a adressé à l'Etat-major des opérations (JSO), avec copie pour information au CTI, une évaluation actualisée des risques qui doivent être pris en compte pour l'établissement du plan de la Défense Militaire du Territoire.

Le passage qui intéresse le Comité R a été rédigé en néerlandais et peut être traduit de la manière suivante :

“(2) menace terroriste en Belgique

(a) Nationale

Depuis le démantèlement des ‘Cellules communistes combattantes’ (CCC) et du ‘Front Révolutionnaire d’Action Proletarienne’ (FRAP) rien ne démontre que la Belgique ne serait plus confrontée à nouveau à des attentats de groupements terroristes nationaux.

(b) Internationale

Sans passer à la mise à l'exécution d'actions terroristes sur notre territoire, il existe en permanence en Belgique des représentants de groupements étrangers qui sont ailleurs actifs dans ce domaine à l'étranger. Le risque existe qu'ils jouent un rôle dans l'organisation et la préparation d'attentats dans les pays qui nous entourent. A ce sujet une vigilance particulière est de rigueur étant donné que les munitions, les explosifs, les armes et l'équipement de nos forces armées peuvent toujours constituer un objectif pour ces groupements.

Bien qu'il n'existe pas d'indication à l'heure actuelle, il n'en demeure pas moins que vu le nombre accru d'interventions de l'armée belge à l'étranger, des actions de revanche soient mises sur pied sur notre territoire avec des objectifs civils ou militaires.

Dans le même contexte le siège des institutions internationales en Belgique représente un but attirant pour les groupements qui ne sont pas d'accord avec le point de vue que la communauté internationale a exprimé par la voix de ces institutions.”

QUATRIÈME COMMENTAIRE

Le Comité R constate que toute allusion à un groupe spécifique de population a disparu.

Le SGR considère de façon objective la présence de groupements étrangers en Belgique.

6.2. Nouveau texte du CTI

Toute référence aux communautés d'immigrés a disparu.

La menace interne peut provenir de n'importe quel individu ou groupement.

La menace potentielle n'est plus décrite.

Les auteurs du document ne reprennent aucun élément qui permettrait de penser que CTI fait autre chose que du renseignement tactique.

Il n'est plus fait mention de la possibilité de contacter des civils ou autres informateurs, si ce n'est avec les services de police.

Le document a donc été nettoyé.

6.3. Approbation du ministre de la Défense nationale

(fin du mois de janvier 1997)

La dernière version du concept de la Défense Militaire du Territoire a été préparée par le Colonel Devleeschouwer et transmise dans un premier stade au chef d'Etat-major des forces armées belges, avant d'être proposée au ministre de la Défense nationale.

7. PEUT-ON PARLER DE LA RÉINSTITUTION DU RÉSEAU STAY-BEHIND ?

Le réseau Stay-Behind mis en place à la suite d'une décision du gouvernement en 1952 avait pour but, en cas d'occupation du territoire belge par un ennemi extérieur, de transmettre des renseignements aux alliés.

Ces renseignements devaient être transmis via des appareils sophistiqués par des civils patriotes formés à l'utilisation de ce matériel en temps de paix.

Ces personnes ont été formées par le SDRA VIII, section du SGR à l'époque.

Rappelons comme il est écrit au point 5.1 du présent rapport qu'une des missions du CTI consiste à protéger militairement le territoire national (cf. 2° de l'art. 15bis §2, 2° de l'A.R. du 13 juin 1995). Cette mission est intitulée Défense Militaire du Territoire (DMT).

L'analyse des documents transmis au Comité R permet d'affirmer que :

- la mission du CTI consiste à protéger des points sensibles du territoire en cas de mobilisation générale;
- cette mission est confiée à des militaires du cadre de réserve afin de décharger les unités de combat;
- en vue de préparer la défense des points sensibles qui leur sont attribués, les officiers de réserve effectuent des missions de renseignement tactique en temps de paix;
- cette mission cesse en cas d'occupation du territoire par l'ennemi;
- les officiers de réserve du CTI ne sont pas entraînés à constituer des réseaux de résistance et de collecte de renseignements en cas d'occupation du territoire. Ils ne disposent pas du matériel qui avait été prévu à cet effet;

- ledit matériel, comme nous le savons, grâce à l'enquête menée au sujet de la réinstauration du réseau Stay-Behind, est entreposé au SGR et n'est jamais mis à la disposition des réservistes;
- la mission du CTI n'est pas une mission du SGR;
- cette mission est également différente de celle des réseaux Stay-Behind qui, eux, devaient entrer en action en cas d'occupation du territoire.

CINQUIÈME COMMENTAIRE

Le Comité R estime que la mission de la Défense Militaire du Territoire ne peut pas être assimilée à la réinstauration du réseau Stay-Behind.

8. CONCLUSIONS

En ce qui concerne l'étude du document controversé

Le Comité R s'interroge sur la nécessité de définir dans ce document une menace actuelle de manière aussi large et générale alors que la mission des réservistes se limite à protéger des points sensibles. Le rôle du CTI n'est pas de faire du renseignement stratégique.

Le Comité R estime qu'il suffit de faire la distinction entre la menace militaire et la menace émanant de groupes terroristes ou subversifs de n'importe quelle origine.

En ce qui concerne l'aspect xénophobe de la définition de la menace

Le Comité R estime qu'associer de manière ambiguë la présence de communautés d'immigrés sur le territoire national à une "menace clandestine à caractère permanent" constitue une atteinte à la dignité des nombreux ressortissants étrangers qui résident dans notre pays.

Une telle vision des choses ne s'inscrit certes pas dans la ligne du programme gouvernemental qui, en son chapitre II.A.3 prévoit que *"la présence stable en Belgique de personnes d'origine étrangère doit être considérée comme un apport positif pour notre société."* Le gouvernement rappelle *"avec insistance qu'il poursuivra la lutte contre toute forme de racisme, d'antisémitisme et de xénophobie"*.

C'est en cela que la note controversée est critiquable.

En ce qui concerne la mission de renseignement du CTI

Le Comité R estime que l'analyse du document controversé et de la déclaration du général Brunin à la presse indique effectivement qu'une structure de réseau de renseignement militaire tactique a été couché sur papier en temps de paix.

Cette structure est indépendante du SGR.

En ce qui concerne l'analyse des dossiers

- Tous les dossiers et documents demandés au colonel Pochet ont été remis au Service d'enquêtes sans réticence.
- Le Service d'enquêtes du Comité R n'a trouvé aucun élément dans ces dossiers qui indiquerait que des informations sont collectées sur des communautés d'immigrés.
- Le Service d'enquêtes n'a trouvé aucun élément dans ces dossiers qui indiquerait que des civils sont utilisés par l'armée en temps de paix comme informateur.
- Les réservistes n'ont pas rempli le chapitre 8 des dossiers établis conformément à la note controversée. Ce chapitre 8 concerne l'"aide possible venant du civil".

En ce qui concerne l'évolution de la rédaction du document controversé

- Le Comité R constate que toute allusion à un groupe spécifique de population a disparu.
- Le SGR a toujours considéré de façon objective la présence de groupements étrangers en Belgique.

En ce qui concerne la réinstauration éventuelle du réseau Stay-Behind

Le Comité R estime que la mission de la Défense Militaire du Territoire ne peut pas être assimilée à la réinstauration du réseau Stay-Behind.

TITRE II : NOS SERVICES DE RENSEIGNEMENT

DEUXIEME PARTIE : LES ENQUÊTES

B. A L'INITIATIVE DU COMITE

CHAPITRE 1 : ENQUETE DE CONTROLE SUR L'UTILISATION D'INFORMATEURS PAR LA SURETÉ DE L'ETAT ET LE SGR

1. PROCÉDURE

Au cours de sa réunion du 23 novembre 1994, le Comité R a décidé d'ouvrir d'initiative une enquête de contrôle sur l'utilisation d'informateurs par la Sûreté de l'Etat et le SGR.

Deux membres du Comité R ont été chargés de suivre cette enquête, de la surveiller et de faire régulièrement rapport au Comité R sur son déroulement.

Conformément à l'article 46 § 3 du règlement d'ordre intérieur, les présidents de la Chambre et du Sénat ont été informés par écrit, le 25 novembre 1994, de l'ouverture de cette enquête.

Le 29 novembre 1994, le chef du Service d'enquêtes a reçu un questionnaire exhaustif le priant d'exécuter l'enquête.

Le 7 décembre 1994, conformément à l'article 43 § 1 de la loi du 18 juillet 1991, le Chef du Service d'enquêtes a informé les ministres de la Justice et de la Défense nationale de l'ouverture de l'enquête.

Le 9 janvier 1995, le Service d'enquêtes a transmis un questionnaire à la Sûreté de l'Etat et au SGR, en les invitant à fournir les réponses au Comité R pour le 15 février 1995.

Seules deux sections du SGR travaillent avec des informateurs, à savoir la section IH (Human Intelligence - en abrégé Humint) et la section CI (Contre-ingérence).

L'administrateur général de la Sûreté de l'Etat a renvoyé le questionnaire complété le 8 février 1995, suivi par le chef du SGR le 14 février 1995.

Pour compléter l'enquête, deux membres du Comité R se sont entretenus avec des responsables des services concernés.

2. FONDEMENT DE L'ENQUÊTE

De toutes les méthodes employées par les services de renseignement pour obtenir des informations secrètes l'utilisation d'informateurs est sans doute la méthode essentielle mais en même temps la plus délicate, aussi bien du point de vue de l'efficacité des services que du respect des droits du citoyen. On n'évoque d'ailleurs cette matière que très rarement.

Le Comité R s'est donné pour objectif de réaliser une étude théorique pour essayer de définir les problèmes que pose le travail avec des informateurs.

Pour ce faire, le Comité R s'est basé sur :

- la doctrine aussi bien nationale qu'internationale;
- des briefings donnés par des agents des services de renseignement;
- l'enquête menée auprès des différents services de renseignement et les contacts avec les responsables de ces services;
- une enquête de contrôle relative à des renseignements fournis par un informateur;
- l'expérience personnelle de certains membres du Service d'enquêtes du Comité R;
- les notes internes des services de renseignement;
- l'enquête parlementaire sur la manière dont a été menée la lutte contre le banditisme et le terrorisme.

Dès le début de ses travaux, le Comité R a décidé de ne pas se faire communiquer de dossiers.

En droit belge, la doctrine s'intéresse très peu à cette problématique.

Monsieur Ch. De Valkeneer dans certains aspects de son livre *"Le Droit de la Police"* (Editions De Boeck - 1991) traite principalement des méthodes policières.

La doctrine étrangère l'étudie par contre de façon approfondie. L'utilisation des informateurs par les services de renseignement, est le thème d'un ouvrage particulièrement intéressant : *"Policing Politics - Security Intelligence and the Liberal Democratic State"* (P. GILL - first published 1994 in Great Britain by Frank CASS and Co. Ltd - Gainsborough House, Gainsborough Road, LONDON E11 1RS, England).

Le Comité R a estimé nécessaire d'évoquer cet important problème et de faire les recommandations utiles en cette matière en raison de ses missions légales qui visent à garantir la protection des droits que la Constitution et la loi confèrent au citoyen, ainsi qu'à veiller à la coordination, et à l'efficacité des services de renseignement.

Le Comité a pu se rendre compte, à l'occasion d'enquêtes antérieures, des problèmes que l'utilisation d'informateurs est susceptible de poser.

L'enquête sur l'utilisation du renseignement fourni par un informateur au SGR (voir rapport annuel 1995, pp. 140 à 142), met clairement en lumière la manière dont un informateur a essayé de faire pression sur un service de renseignement.

3. L'INTÉRÊT PORTÉ AU PROBLÈME PAR LE PARLEMENT

Le rapport de l'enquête parlementaire sur l'organisation de la lutte contre le banditisme et le terrorisme, contient quelques passages relatifs aux méthodes de collecte d'informations par la Sûreté de l'Etat et, en particulier, aux informateurs.

- *"Il ressort des témoignages qu'il n'existe aucun code déontologique ni aucune réglementation stricte à la Sûreté en ce qui concerne la collecte d'informations".*
En règle générale, les agents de la Sûreté n'entrent pas directement en contact avec le milieu à surveiller. La Sûreté collecte les informations par le biais d'informateurs rémunérés qui sont

en contact étroit avec le milieu observé et qui travaillent sur ordre des agents de la Sûreté (le service extérieur).

Aux dires des témoins, la provocation et la diffamation sont des techniques tout à fait exclues. Selon l'administrateur-directeur-général, l'infiltration n'est pratiquée que très exceptionnellement mais elle n'est pas rejetée par principe. On ne sait que peu de choses au sujet de la collaboration avec les P.T.T. Les écoutes téléphoniques sont toujours interdites par la loi ⁽¹⁾.

- *"Compte tenu de l'organisation de la Sûreté de l'Etat, telle qu'elle ressort de témoignages, on peut se demander comment le service d'études de celle-ci qui ne rencontre jamais lui-même les informateurs, est en mesure d'évaluer les informations fournies. La vérification de la fiabilité des informateurs et des informations qui leur sont communiquées posent manifestement un problème".*
- *"Les témoignages ne permettent toutefois pas de déterminer avec précision qui avait donné l'ordre d'infiltrer le WNP. Aucun ordre spécifique d'infiltrer ce groupement à une date déterminée n'aurait jamais été donné. L'administrateur-directeur-général prétend d'ailleurs que la Sûreté de l'Etat ne procède pas de cette manière. Il déclare que c'est à lui seul qu'il appartient de définir les objectifs. Leur opérationnalisation relève de la compétence des supérieurs hiérarchiques des services extérieurs. Les témoins affirment cependant que l'ordre d'infiltration a été donné directement par l'administrateur-directeur général. Il avait l'habitude de donner directement ses ordres aux fonctionnaires subalternes sans suivre la voie hiérarchique ⁽¹⁾."*

On ne trouve ici aucune allusion aux informateurs du SGR.

Le Comité R a également pris connaissance des questions parlementaires posées par :

- ? Monsieur Van Dienderen (AGALEV) au ministre de la Défense nationale le 8 juillet 1988
question 35 - Questions et Réponses - Chambre 1987-1988, p. 2094;
et le 25 novembre 1988 - question 110 - Questions et Réponses, Chambre 1988-1989, p. 3297;
- ? Monsieur Nols (PRL) au ministre de la Justice le 6 janvier 1989 - question 133 - Questions et Réponses, Chambre 1988-1989, p. 3992, relative aux activités de la Sûreté de l'Etat dans le milieu des étudiants zaïrois;
- ? Le député Monsieur Sleenckx au ministre de la Défense nationale :
"Gendarmerie - Transmission de renseignements au service de sécurité militaire SGR"
(Questions et Réponses - Chambre - 8 septembre 1989 - question 430 - p. 6914);
- ? Le député Monsieur Didden au ministre de l'Intérieur: "Gendarmerie- Indicateurs" (Questions et réponses - Chambre des Représentants - 3 octobre 1995 - question 83 - p. 911);
- ? Monsieur Ceder (VB) au ministre de la Défense nationale :
"Activités des services de renseignements militaires dans les universités"
(Sénat - Sommaire - 9 novembre 1995 - question orale - p. 96);

⁽¹⁾ Enquête parlementaire sur la façon dont est organisée la lutte contre le banditisme et le terrorisme, troisième partie, pp. 285-286

⁽²⁾ Voir enquête citée au renvoi ⁽¹⁾, troisième partie, pp. 287, 288 et 289.

- ? M. Boutmans (AGALEV) au ministre de l'Intérieur :
 "Gendarmerie - Maintien de l'ordre - Collecte d'informations"
 Réponse du Ministre :
 " ..Le recours à des informations, ou dans certains cas, à des indicateurs est un procédé autorisé... Le recours à des indicateurs doit se faire conformément à la loi ... "
 (Questions et réponses - Sénat - 16 juillet 1996 (n° 1-23) - question 139 du 3 mai 1996);
- ? Monsieur Boutmans (AGALEV) au ministre de la Justice:
 "Sûreté de l'Etat - Récolte d'informations"
 De quelle manière et dans quelles circonstances peut-on avoir recours à des informateurs, qui peut être choisi comme informateur, sous quel contrôle, etc...
 Réponse du Ministre: " (...) Il est fait appel à des informateurs, lorsque les renseignements ne peuvent pas être obtenus par d'autres moyens.(...)"
 (Questions et réponses - Sénat - 16 juillet 1996 - question n° 157 du 24 mai 1996);
- ? Commission de la Justice: demande d'explications de Madame Milquet (PSC) au ministre de la Justice sur "les informateurs".
 Intervenants: Madame Milquet, Monsieur Desmedt, le Ministre de la Justice;
 (Sénat - Débats de la séance publique de la Commission - séance du 21 janvier 1997 - Débats parlementaires du Sénat - COM1-80)

4. CONSIDÉRATIONS PRÉLIMINAIRES

Il convient de distinguer les informateurs d'un service de police de ceux d'un service de renseignement (voir plus loin la comparaison avec les services de police et leurs directives).

Il ressort des deux ouvrages cités ci-dessus que l'utilisation d'informateurs pose des problèmes déterminés (aussi bien pour les services de police que pour les services de renseignement) et comporte un certain nombre de risques, relatifs entre autres :

- au respect de la vie privée;
- au risque que les informateurs puissent commettre des infractions pénales;
- au danger de provocation et de manipulation par l'informateur;
- au système de recrutement des informateurs;
- à l'intégrité physique de l'informateur.

4.1. Définition d'un informateur

Il n'existe pas en Belgique de définition légale de "l'informateur".

Le dictionnaire Petit Robert définit l'informateur comme une *"personne qui fournit des informations"*.

Les différents services tentent de donner une définition des informateurs. Les mêmes éléments reviennent souvent.

Le Comité R propose la définition suivante d'un informateur :

- une personne qui, rémunérée ou non, sollicitée ou spontanée, fournit des informations difficilement accessibles par d'autres voies et peut de ce fait encourir un risque matériel, moral ou physique.

Le livre de P. GILL renvoie à un classement des informateurs.

Ce classement des informateurs est donné par la Commission Mac. Donald (*Commission of inquiring concerning certain activities of the Royal Canadian Mounted Police*).⁽¹⁾

Elle distingue 4 catégories principales d'informateurs :

- informateur spontané : un citoyen ordinaire fournit une information unique sans aucune contrepartie. Dans ce classement interviennent aussi des personnes qui fournissent une information dans le but d'en retirer un avantage.
- informateur occasionnel non suivi : un citoyen qui est encouragé à fournir une information dont il a eu connaissance fortuitement dans l'exercice de sa profession, par ex. un chauffeur de taxi, le personnel d'entretien, etc... Cette source n'est pas rémunérée. Son équivalent auprès du FBI correspond à la "confidential source" utilisée dans 50 % des cas pour obtenir des renseignements à l'intérieur du pays (suivant l'étude réalisée par "the General Accounting Office, US Congress"⁽¹⁾ (GAO)).
- informateur suivi : il est régulièrement contacté et sollicité pour recueillir des informations. Cette source est rémunérée.
- informateur qui infiltre à long terme: cette source peut soit faire partie d'une organisation sur laquelle elle est disposée à fournir des informations, soit être membre d'un service de renseignement et s'infiltrer dans l'organisation sous une fausse identité. Une étude faite sur le FBI (par le GAO) révèle que 85 % des renseignements à l'intérieur du pays proviennent des deux dernières catégories d'informateurs.

On retrouve plus ou moins le même classement auprès des services de renseignement belges.

La loi, dans certains pays, permet aux membres des services de renseignement d'infiltrer sous une fausse identité certains groupements à surveiller (voir entre autres Undercover and Sensitive Operations Unit - Attorney General's Guidelines on FBI - revised 13 novembre 1992)⁽¹⁾

C'est une différence essentielle avec la situation en Belgique.

⁽¹⁾ Commission of Enquiry Concerning Certain Activities of the Royal Canadian Mounted Police (hereafter Mc Donald), First Report, Security and Information (1979), Second Report, Freedom and Security under the Law (1981), and Third Report, Certain RCMP Activities and the Question of Governmental Knowledge (Ottawa : Minister of Supply and Services, 1981).

⁽²⁾ Church Committee, Final Report, Book III, Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans (Washington DC : US Government Printing Office, 1976).

⁽³⁾ Les règles contenues dans ce document sont d'application pour toutes les enquêtes menées par le FBI, à l'exception de celles menées dans le cadre de ses responsabilités en matière de contre-espionnage étranger et de sa responsabilité en matière de renseignements étrangers (traduction libre).

Dans la suite de l'enquête, on étudie de plus près les différentes catégories d'informateurs aussi bien à la Sûreté de l'Etat qu'au SGR.

4.2 La nécessité d'informateurs

Les informateurs sont essentiels pour les services de renseignement. Ils constituent la base de travail du renseignement.

On attend d'un service de renseignement qu'il soit en mesure d'informer de manière objective les autorités sur les dangers potentiels ou réels pour l'intégrité et la pérennité des institutions démocratiques d'un pays.

La mission des services de renseignement implique que, systématiquement et sur une période suffisamment longue, des renseignements soient recueillis sur des personnes ou des groupements dont on sait ou dont on croit qu'ils peuvent, dans le contexte social et politique existant, constituer une menace pour la sûreté intérieure ou extérieure de l'Etat.

L'information recueillie par les services de renseignement est généralement à l'état brut, de fiabilité douteuse, mais une analyse minutieuse peut la transformer en renseignement qui, bien que parfois encore incertain, peut être utile aux décideurs politiques.

Il s'agit d'une problématique très délicate et complexe, en raison de l'importance des relations humaines dans les contacts entretenus entre agents et informateurs.

De plus, les missions légales des services de renseignement ne sont toujours pas définies par la loi.

Il ressort de l'enquête parlementaire sur la manière dont est organisée la lutte contre le banditisme et le terrorisme que :

"il n'existe aucun code déontologique ni aucune réglementation stricte à la Sûreté en ce qui concerne la collecte d'informations" (voir point 3 ci-dessus).

4.3. Risques liés au travail avec des informateurs

Suivant l'ouvrage précité de P. GILL, le travail avec des informateurs présente certains avantages, surtout si on le compare avec les moyens techniques de surveillance.

La collecte d'informations par le biais d'informateurs est généralement plus économique que l'utilisation de moyens techniques comme par exemple les écoutes téléphoniques. Cette méthode de recueil des informations est plus souple et plus intense.

Néanmoins, les risques liés au travail avec des informateurs sont très nombreux.

- Les informateurs rémunérés auront facilement tendance à surestimer leur information afin d'en retirer un plus grand profit matériel.
- Les motivations des informateurs peuvent être de différentes natures telles que, par exemple la vengeance, l'envie, le repentir, l'argent, etc..., avec la conséquence qu'il sera très difficile

d'évaluer à sa juste valeur l'information obtenue.

- Celui qui recrute l'informateur peut avoir tendance à se montrer trop optimiste quant à sa fiabilité et ce, par intérêt personnel.
- Travailler avec des informateurs comporte aussi des risques de tromperie et de trahison, qui peuvent à la longue laisser des traces sur le plan moral, aussi bien auprès de l'informateur qu'auprès du recruteur, ce qui peut finalement avoir des suites néfastes en ce qui concerne l'efficacité et l'éthique du service.
- Une collaboration à long terme peut parfois créer des liens étroits entre le recruteur et l'informateur, avec pour conséquence que les services aussi bien que leurs membres peuvent devenir très réticents à partager leurs sources. Cela peut entraîner des conséquences très néfastes sur la coordination des opérations à l'intérieur d'un même service et d'autant plus lorsqu'il s'agit de collaboration avec d'autres services.
- Il arrive que l'informateur se comporte en agent provocateur. Sa vie peut alors être menacée.
- Ici, se pose alors le problème de la protection de l'informateur. P.GILL cite dans son livre l'affaire Kenneth Lennon qui s'est passée au Royaume-Uni et à propos de laquelle une certaine documentation a pu être retrouvée. A la demande de la "Special Branch", Lennon a infiltré un team de "l'IRA" au début des années septante et a dû être poursuivi pénalement afin de pouvoir conserver sa couverture. Il fut acquitté et quelques jours plus tard, le "National Council for Civil Liberties" a prétendu qu'il avait été forcé de se comporter en agent provocateur. Il fut retrouvé mort trois jours plus tard, vraisemblablement abattu par l'IRA. Une première enquête menée par la police de Londres a fait apparaître qu'il n'existait aucune preuve permettant d'affirmer que Lennon ait été contraint d'agir en informateur d'abord, en agent provocateur ensuite.

On n'a pas pu démontrer que des agents de la "Special Branch" avaient outrepassé leurs directives, ni qu'ils portaient une responsabilité directe ou indirecte dans la mort de Lennon. L'opinion que la "Special Branch" avait influencé de manière incorrecte l'arrestation et le procès de Lennon n'a pu être établie.

Geoffrey Robertson dans son ouvrage intitulé *"Reluctant Judas: the life and death of the Special Branch informer, Kenneth Lennon"*⁽¹⁾, aboutit à de toutes autres conclusions.

La "Special Branch" avait lavé Lennon de toute responsabilité dans les délits graves qu'il avait commis et reconnus. Elle nia qu'il serait intervenu comme agent provocateur et aurait incité des agents agitateurs politiques à se livrer à des activités criminelles qu'ils n'auraient pas commises autrement. Elle laissa la presse répandre de fausses informations. Elle cacha des pièces à conviction aux avocats dans deux importants procès criminels.

La "Special Branch" a fait usage de procédures criminelles pour sauvegarder la couverture de son informateur, mais lorsque les choses tournèrent mal et que l'informateur fut démasqué, elle n'a pas réussi à le protéger.

La différence entre les deux versions de l'affaire Lennon s'explique par le fait que l'information, au fur et à mesure de sa transmission dans la hiérarchie, avait été "expurgée".

En raison de cette expurgation, l'enquête ne pouvait conclure que les directives avaient été

⁽¹⁾ London : Temple Smith 1976

outrépassées dans cette affaire. ⁽¹⁾

- P. GILL aborde également la manière dont les services de renseignement recrutent leurs informateurs.

Les services de police recrutent souvent leurs indicateurs en concluant un accord avec des personnes arrêtées.

Les services de renseignement ne disposent pas de compétences policières, comme par exemple le CSIS (service de renseignement canadien), le Security Service en Angleterre (les services de renseignement belges ne possèdent pas non plus de compétences policières), ils doivent dès lors employer d'autres techniques pour recruter leurs informateurs.

Suivant l'auteur, le moyen de pression le plus important dont disposent les services de renseignement est la manipulation à l'occasion d'enquêtes de sécurité ou de procédures d'immigration. L'usage de tels procédés peut cependant porter sérieusement atteinte aux droits des citoyens.

En ce qui concerne les services de renseignement et de police belges, Monsieur De Valkeneer énumère des risques semblables, notamment :

- des infractions pénales commises par l'informateur qui infiltre.

"L'infiltration d'un milieu est souvent une opération complexe. Elle suppose que l'agent entre en contact avec un certain nombre de personnes, qu'il entretienne avec elles des rapports suffisamment étroits et qu'il garde le secret sur la finalité de son activité. Une manière efficace de surmonter ces différentes difficultés peut consister, notamment, en une participation directe à l'activité délinquante du milieu infiltré. Cela peut même être une nécessité pour se faire réellement accepter.

- le danger de provocation et de manipulation.

Dans le cadre des informateurs de la Sûreté de l'Etat, l'auteur cite l'exemple de l'affaire "Pourbaix", dans laquelle la Cour d'Assises du Hainaut a rendu un arrêt en 1889.

27 personnes appartenant au parti socialiste républicain étaient accusées de complot contre la sûreté intérieure de l'Etat, pour avoir commis plusieurs attentats à la dynamite dans la région de La Louvière et appelé à la grève générale.

Les débats devaient révéler que les instigateurs de cette agitation n'étaient autres en réalité que des agents à la solde de la Sûreté de l'Etat. Deux d'entre eux - Pourbaix et Laloi - furent condamnés quelques mois plus tard par la même juridiction, à deux ans de prison.

- En ce qui concerne le recrutement des informateurs, l'auteur se demande si la Sûreté de l'Etat n'exerce pas de pression sur des personnes pour obtenir des informations :

"Il est théoriquement exclu que des agents de la sûreté exercent des pressions sur des personnes afin qu'elles acceptent de fournir certaines informations. Ce genre de pratique n'aurait pas lieu et aucune interférence ne se produirait avec des affaires judiciaires"⁽¹⁾

⁽¹⁾ Traduction libre

⁽²⁾ Question n° 133 de Monsieur Nols du 6 janvier 1989, Bull - Questions et réponses - Chambre - 1988-1989, p.3992 concernant l'activité d'agents de la Sûreté au sein de milieux d'étudiants zairois (traduction libre du texte précité)

Le Comité R est d'avis que cette problématique soulève des problèmes éthiques et juridiques.

4.4. Solutions proposées à l'étranger pour remédier à ces risques⁽¹⁾

Selon P. GILL, la question de savoir comment résoudre ces problèmes n'a été abordée qu'en Amérique du Nord.

Situation en Amérique du Nord

En 1976, l'Attorney General LEVI (Ministre de la Justice) a édicté et publié des directives relatives à l'utilisation d'informateurs par le FBI, dans le cadre de l'exécution des missions tant en matière de sûreté intérieure qu'en matière pénale. Le FBI doit clairement expliquer à ses informateurs que:

- ils ne doivent pas être impliqués dans des actes de violence;
- ils ne peuvent pas faire appel à des méthodes illégales pour obtenir des informations;
- ils ne peuvent pas concevoir d'actes criminels;
- ils ne peuvent pas prendre part à des activités criminelles.

Lorsque le FBI apprend qu'un de ses informateurs est impliqué dans un délit, il doit le porter à la connaissance des services de police compétents ou, si cela n'est pas opportun, au département de la Justice.

Le "Church Committee (Senate Select Committee to study governmental operations with respect to intelligence activities)" propose des règles plus sévères. Ainsi le FBI ne peut recruter de nouveaux informateurs ou charger des informateurs déjà recrutés d'une nouvelle mission, sauf si un rapport écrit de l'"Attorney General" précise que des techniques moins pénétrantes ont été envisagées et rejetées. Dans ce cas, le recours à un informateur est indispensable pour obtenir le renseignement.

Le "Church Committee" a rejeté une proposition qui préconisait qu'une ordonnance écrite d'un juge autorise le recrutement d'un informateur. Le "Church Committee" estime que les juges seraient alors trop impliqués dans l'instruction de l'affaire et que cette procédure constituerait une étape vers un système inquisitorial. La Commission McDonald a partagé cet avis (voir supra). La Commission recommande que les directives administratives soient étayées, approuvées par le ministre et publiées.

Suivant cette recommandation, ces directives devraient spécifier que les informateurs ne doivent pas être mêlés à des activités illégales, ne doivent pas jouer les agents provocateurs ou être utilisés pour provoquer des troubles, excepté en cas d'espionnage, de sabotage ou d'immixtion extérieure.

Situation au Canada

Les "CSIS Act Guidelines" ne sont pas publiées. Le Gouvernement a fait savoir qu'elles sont

⁽¹⁾ Selon l'ouvrage cité plus haut de P.GILL

basées sur les critères suivants :

- des sources humaines ne seront utilisées que dans la mesure où c'est raisonnable et nécessaire dans le cadre des responsabilités statutaires du service;
- la nécessité de recourir à une source doit être minutieusement pesée par rapport aux préjudices possibles qui pourraient porter atteinte aux libertés civiles;
- un contrôle est indispensable en raison du caractère contraignant de la méthode;
- les informateurs doivent exécuter leurs tâches sans être impliqués dans des pratiques illégales. Ils doivent veiller à ce que leur comportement ne jette pas le discrédit sur le service ou le gouvernement canadien;
- les informateurs doivent être traités de façon à ce que la protection de leurs activités opérationnelles et leur sécurité personnelle soient garanties;
- les informateurs doivent être traités avec une certaine éthique et loyalement aussi bien dans leur accompagnement qu'en ce qui concerne leur rémunération;

Contrairement aux techniques d'écoutes pour lesquelles une autorisation juridique est nécessaire au Canada et aux Etats-Unis, l'utilisation d'informateurs et leur contrôle est de la seule compétence des services de renseignement. Seul un contrôle interne est prévu.

Certains services de renseignement se sont opposés aux initiatives qui tentaient d'imposer un contrôle externe sur l'efficacité des informateurs ⁽¹⁾.

Selon P. GILL, la problématique de l'utilisation d'informateurs par les services de renseignement reste incontrôlable et ne semble pas pouvoir faire l'objet d'étude approfondie en raison du fait qu'elle n'a pas pour objectif la recherche et la poursuite d'infractions.

5. PORTÉE DE L'ENQUÊTE

L'enquête de contrôle sur l'utilisation des informateurs par les services de renseignement belges porte plus particulièrement sur les points suivants :

- a) les différentes sortes d'informateurs;
- b) les directives qui sont d'application;
- c) le mode de recrutement des informateurs;
- d) les missions des informateurs;
- e) la rémunération des informateurs;
- f) l'évaluation des informateurs;
- g) la protection des informateurs;
- h) les circonstances dans lesquelles les services de renseignement mettent fin à la collaboration avec des informateurs;
- i) comparaison avec les services de police et leurs directives.

⁽¹⁾ See T. Poveda, lawlessness and reform: the FBI in transition (Pacific Grove, CA : Brooks/Cole Publishing, 1990) p. 83 regarding the FBI's refusal of a request from the GAO (General Accounting Service) to carry out such an audit.

Comme indiqué supra, les informateurs constituent la base du recueil de l'information. Toute indiscretion doit être bannie pour sauvegarder l'efficacité du service. Ce sujet doit donc être traité avec la plus grande circonspection.

En application de son règlement d'ordre intérieur, notamment l'article 66, le Comité R a tenu compte, en publiant son rapport, des éléments suivants :

- le préjudice qui pourrait être causé au bon fonctionnement des services de renseignement nationaux et étrangers;
- la protection de la vie privée et de l'intégrité physique des personnes;
- la coopération internationale entre les différents services;
- le droit des citoyens de s'assurer du bon fonctionnement des services de renseignement.

En conséquence, le Comité n'a rendu, que partiellement publics, les résultats de cette enquête, afin de ne pas compromettre le bon fonctionnement des services et la confiance que les informateurs placent en eux.

a) Sortes d'informateurs

Comme déjà mentionné ci-dessus (*cf. 4.1*), on distingue différentes sortes d'informateurs, à savoir ceux qui sont utilisés occasionnellement et les informateurs enregistrés recrutés pour une période déterminée et qui fournissent régulièrement des informations sur les matières qui intéressent les services de renseignement.

On retrouve cette distinction tant à la Sûreté de l'Etat qu'au SGR.

b) Les directives applicables

La problématique des informateurs n'est régie par aucune norme en Belgique (ni loi, ni arrêté royal ou ministériel).

A la Sûreté de l'Etat :

Depuis 1947, 53 ordres de service concernent directement ou indirectement les informateurs.

Chronologie

40 documents rédigés jusque fin 1965;
6 documents rédigés entre 1966 et fin 1975;
5 documents rédigés entre 1976 et 1985;
2 documents rédigés entre 1986 et 1995.

Thèmes

- Affectation des fonds spéciaux ;

- Contrôle;
- Protection des informateurs;
- Rédaction des rapports;
- Précautions à prendre;
- Collaboration avec la gendarmerie;

La note générale du 13 février 1980, qui doit régler toute la matière des "sources de la Sûreté de l'Etat", traite en grande partie du financement des sources.

Au SGR / IH (Humint) :

Il n'existe aucune directive écrite, mais des formulaires sont utilisés.

Au SGR / CI (Contre-Ingérence):

Toute la matière concernant les informateurs est réglée par la note de service du 14 février 1995. Il s'agit d'une note provisoire. De nouvelles directives qui insistent notamment sur une meilleure évaluation des informateurs, par le biais de leur contrôle, sont en préparation.

c) Mode de recrutement des informateurs

Le mode de recrutement des informateurs, qui n'est pas toujours consignée dans des notes de service, diffère suivant les services de renseignement. Chaque service utilise une méthode déterminée. Les services font une distinction entre informateurs occasionnels et enregistrés.

La revue Politeia (revue professionnelle de la police belge) d'octobre 1996 a publié une interview de l'administrateur général de la Sûreté de l'Etat, qui déclare à ce sujet :

"Avant que quelqu'un ne soit accepté comme informateur, une enquête de sécurité est effectuée et le casier judiciaire de la personne concernée est contrôlé. Nous sommes sévères en cette matière. Quelqu'un qui, dans le passé s'est rendu coupable d'escroquerie, de vol avec effraction, est en principe refusé. Par contre, la plupart des bons informateurs de police ont (et c'est inévitable) des antécédents judiciaires. En ce qui concerne le mode de recrutement, il n'existe pas de schéma fixe. Il arrive que des personnes se présentent simplement chez nous, par le biais d'un coup de fil ou d'une lettre, et que nous constatons au cours de l'entretien qui s'ensuit que la personne dispose en effet d'informations intéressantes. Cette façon de travailler peut parfois déboucher sur de très bons résultats. Il arrive aussi que nous approchions - par exemple lors de réunions spéciales - des personnes avec lesquelles nous tentons d'établir une relation de confiance qui débouche sur des informations. Ces derniers temps, les services de police nous envoient aussi régulièrement des informateurs, ce qui est une preuve des bons rapports que nous commençons à entretenir. Auparavant, cela ne se serait jamais produit. Dans le monde du renseignement, il existe même des informateurs qui collaborent au niveau européen avec différents services. En général, j'estime que le développement de notre système d'informateurs se fait de manière plus stratégique que celui des services de police. Les services de police, par contre, disposent d'autres sources d'information efficaces qui ne sont pas directement accessibles à la Sûreté de l'Etat".

d) Missions des informateurs

A la Sûreté de l'Etat :

Le service recherche ponctuellement des informateurs susceptibles de lui fournir des informations relatives à la "liste des sujets". On utilise les informateurs dans tous les sujets classiques. Certaines priorités sont fixées, mais elles peuvent être modifiées suivant les circonstances.

La recherche sélective d'informateurs basée sur la liste des sujets est une fonction générale et permanente de la Sûreté de l'Etat : c'est son essence même.

A propos de la criminalité organisée, l'administrateur général a déclaré dans l'interview citée plus haut :

"La Sûreté de l'Etat veut faire de la lutte contre la criminalité organisée une de ses priorités principales. Il est toutefois encore trop tôt pour définir en détail la manière dont la Sûreté de l'Etat peut et souhaite fournir une contribution dans ce domaine.

Actuellement, nous tâtons encore un peu le terrain pour voir ce qui s'y passe. Nous n'avons commencé qu'au début de 1995 à travailler de manière systématique sur la problématique de la criminalité organisée. Au départ, certains membres du personnel ne se sentaient pas très sûrs d'eux, parce qu'ils ne savaient pas trop bien comment procéder. Cette phase a été dépassée lorsque, d'une façon assez naturelle, on a trouvé des points d'attache avec d'autres matières que le service traitait depuis longtemps. Nous en sommes maintenant à commencer à y voir clair dans certains secteurs - même si pas tous - de la criminalité organisée et surtout de celle des pays de l'Europe de l'Est.

En ce moment, nous travaillons sur une affaire où - je pense que cela constitue un fait nouveau - des liens matériels sont clairement établis entre plusieurs importants réseaux criminels. Il s'agit donc d'un phénomène extrêmement inquiétant de constitution de "cartel", qui, à mon sens, prendra encore de l'importance à l'avenir".

Au SGR / IH

Le SGR recrute des informateurs en vue de la collecte et/ou de la recherche d'informations sur l'étranger suivant des thèmes prioritaires.

Au SGR / CI

Les agents de la section contre ingérence recherchent ponctuellement des informateurs susceptibles de fournir des informations concernant une "liste de sujets" établie par les responsables de la section.

e) La rémunération des informateurs

Les autorités fiscales et sociales ne sont pas tenues au courant des versements opérés en faveur des informateurs de manière à garantir de leur anonymat.

Les deux services de renseignement belges gèrent la manière de rémunérer les informateurs de façon plus ou moins analogue. Il importe cependant de constater qu'aucun barème n'est prévu.

Dans des cas exceptionnels, la possibilité de payer des montants élevés existe, sans qu'aucune tarification ne soit prévue à ce sujet.

Le problème se pose avec d'autant plus d'acuité aux services de renseignement qu'eux-mêmes ne disposent d'aucune circulaire ministérielle en la matière (ce qui est le cas pour les services de police, bien que les circulaires ne prévoient pas non plus de tarification). Dans d'autres pays, par exemple aux USA, ce problème est minutieusement réglé.

A la Sûreté de l'Etat

L'administrateur général a communiqué les montants versés aux informateurs durant l'année 1996. Cette information est secrète mais a néanmoins été communiquée au Comité R à sa demande. Le surplus du budget 1996 a été reversé au Trésor.

Les informateurs sont le plus souvent payés en fonction des prestations fournies et des frais exposés. Ces montants sont toujours limités. Ils sont payés sur proposition de l'agent de renseignement après examen de sa hiérarchie et moyennant l'accord final de l'administrateur général.

Plus du tiers des ordres et notes de service concernent l'utilisation des fonds. Certaines directives traitent du montant maximum des indemnités qui peuvent être payées à certaines catégories d'informateurs.

Au SGR

Le chef du SGR a communiqué les montants versés aux informateurs durant l'année 1996. Cette information est secrète mais a néanmoins été communiquée au Comité R à sa demande. Les fonds non utilisés ont été reversés au Trésor.

Au SGR / IH

La plupart du temps, les informateurs ne reçoivent que le remboursement de leurs frais, mais ils peuvent également percevoir une indemnité.

On applique différents critères, tels que l'opportunité des informations fournies, les risques encourus par la source, les possibilités financières du service, etc...

La décision appartient en dernier ressort au chef du SGR / IH, sur proposition et en concertation avec les autorités hiérarchiques de la section IH.

Au SGR / CI

Parmi les informateurs rémunérés, certains perçoivent un montant mensuel fixe et le remboursement de leurs frais, alors que d'autres ne reçoivent que le remboursement de leur frais.

Le critère retenu est la valeur de l'information qu'ils apportent. Les sommes payées sont fixées par le chef de section en concertation avec et sur proposition d'autres responsables de la section CI.

Aucune directive n'en limite les montants.

La comptabilité est mensuellement contrôlée par le chef de section.

f) Évaluation des informateurs

A la Sûreté de l'Etat

Différents ordres de service traitent du contrôle et de l'évaluation des informateurs.

Les services extérieurs et les analystes se concertent en permanence. Ces derniers signalent lorsque l'information fournie diffère régulièrement de l'information reçue par d'autres sources (aussi bien publiques que confidentielles).

Chaque informateur fait annuellement l'objet d'un rapport. Sur base de ce rapport, il peut être proposé de réduire ou d'augmenter sa rémunération mais aussi de le rayer des listes des informateurs rémunérés.

Au SGR / IH

Les dossiers fournis par l'informateur et l'informateur lui-même sont évalués annuellement.

La section Humint (IH) et la section exploitation (EI) s'échangent en permanence des informations.

Au SGR / CI

Les analystes procèdent à une évaluation permanente des informations fournies et les classent en fonction de leur valeur et de leur exactitude par comparaison avec d'autres sources.

Chaque informateur fait l'objet de deux rapports d'évaluation par an. Ces rapports sont discutés avec le chef du SGR/CI qui prend la décision finale.

g) La protection des informateurs

A la Sûreté de l'Etat

Avant 1965, la protection des informateurs avait fait l'objet de six ordres et notes de service, qui insistent toutes sur la nécessité de conserver à tout prix l'anonymat des informateurs, particulièrement dans la rédaction des rapports d'information.

Il y a une protection directe de l'identité des informateurs et en ce qui concerne les informations recueillies respect du danger encouru par les "sources".

La sécurité des informateurs, essentielle pour la bonne marche du service, est assurée de manière stricte.

S'il s'agit d'un informateur dont l'identité doit être particulièrement protégée, les rapports doivent porter une mention supplémentaire : " danger source".

Cependant, on peut affirmer que la protection de l'anonymat d'un informateur lui incombe en premier lieu. Indiscrétion, imprudence... ont déjà joué bien des tours à maints informateurs.

La Sûreté de l'Etat ne dispose pas de base légale pour protéger ses sources.

Au SGR / IH

L'identité de l'informateur n'est connue que de quelques membres de la section IH. Les informations fournies par l'informateur sont conservées et archivées sous son identification codée.

Au SGR / CI

L'identité de l'informateur est protégée. Elle n'est JAMAIS divulguée. Les contacts entre l'agent du SGR et l'informateur sont entourés de mesures de précaution nécessaires.

h) Les circonstances dans lesquelles les services de renseignement mettent fin à la collaboration avec des informateurs

Chaque service peut décider de mettre fin à sa collaboration avec un informateur pour diverses raisons :

- l'informateur souhaite lui-même cesser la collaboration;
- l'informateur ne présente plus beaucoup d'intérêt pour le service;
- l'informateur n'est pas fiable;
- l'informateur est mêlé à des affaires douteuses;
- indiscrétion, etc...

i) Comparaison avec les services de police et leurs directives

Il faut faire une distinction entre les informateurs des services de police et ceux des services de renseignement.

Tant les missions que les compétences diffèrent.

i.1 Nature de la mission

La mission de la police (mission judiciaire) est définie comme suit par l'article 8 du Code d'Instruction criminelle.

- "La police judiciaire recherche les crimes, les délits et les contraventions, en rassemble les

preuves, et en livre les auteurs aux tribunaux chargés de les punir."

Lorsque, dans ce contexte, des informateurs sont utilisés, il s'agit de personnes qui, sur base des motivations les plus diverses, une seule fois ou sur une longue période, rémunérées ou non, livrent des informations sur des délits commis ou à commettre. La mission est ici clairement définie.

La mission implique que, systématiquement et sur une période suffisamment longue, des informations soient rassemblées sur des personnes ou des groupements dont on sait ou dont on soupçonne qu'ils constituent ou pourraient constituer, dans le contexte social et politique existant, une menace pour la sécurité interne ou externe de l'Etat.

C'est une matière très subtile dont les buts ne sont fixés que de manière générale.

Dans l'interview parue dans "Politeia", l'administrateur général de la Sûreté de l'Etat a déclaré:

"Les services de renseignements quels qu'ils soient, sont enclins à regarder les choses à terme, voire à long terme. Le résultat immédiat est moins important que la pénétration dans (contrairement à la pratique des services de police, ont fait toujours appel à des tiers qui ne font pas partie du service) certaines structures que l'on vise à connaître. Par contre, les services de police sont confrontés à la nécessité de rechercher certaines infractions et d'intervenir rapidement. Il est toutefois clair qu'ils sont en train d'évoluer en cette matière et qu'ils souhaitent se rapprocher, en ce qui concerne les objectifs et les techniques, des services de renseignements : ils commencent aussi à s'attacher davantage à la mise en lumière de structures. En tant que méthode d'investigation systématique, cette démarche est nouvelle pour les services de police, alors que pour les services de renseignements, il s'agit de la méthode de travail classique.

D'autre part, et même si l'on fait abstraction de la discussion actuelle relative aux modalités de la recherche dite "proactive" (en fait, il faut parler de recherches "pré-actives", il est et il reste de fait que, dans la plupart des cas, les services de police seront appelés à continuer à agir de façon ponctuelle, c'est-à-dire à l'occasion des (très nombreuses) infractions découvertes d'office ou suite à une plainte".

"La Sûreté de l'Etat agit à partir d'une optique totalement différente de celle des services de police; nous ne nous concentrons en effet pas sur la recherche systématique des infractions pénales, mais nous cherchons à mettre en lumière certains réseaux et structures. Pour ne donner qu'un exemple de cette approche, il suffit de renvoyer la problématique des sectes nuisibles. Celles-ci se positionnent dans une zone d'ombre que l'on ne peut pas situer de prime abord dans le cadre des activités policières. Il est en effet très difficile d'établir a priori si de telles sectes s'adonnent à des activités criminelles, parce que, sur ce plan, elles prennent soigneusement leurs précautions. Elles disposent souvent d'une équipe de collaborateurs juridiques et savent donc "jusqu'où elles peuvent aller". La seule manière de combattre efficacement les sectes consiste à obtenir avant tout une image précise de leur structure et de leurs mécanismes de fonctionnement, y compris sur le plan financier et de vérifier ensuite si des infractions n'ont pas été commises. Il faut veiller à ne pas réagir tout de suite de manière répressive, sauf dans les cas où cela s'imposerait vraiment".

Le mode de travail classique des services de police en cette matière est souvent, trop fragmentaire. Jusqu'à présent, les services de police se sont généralement limités à rassembler des bouts d'information, la plupart du temps à la suite de plainte individuelles, déposées par des parents de membres des sectes et qui ne fournissent aucune information utile relative à d'éventuels éléments constitutifs d'infractions

J'espère qu'à l'avenir il sera possible d'arriver à ce que le contenu de tels dossiers soit automatiquement communiqué par les parquets à la Sûreté de l'Etat, qui sera dès lors en mesure de compléter sa banque de données centrale, qui existe déjà, et de la mettre à la

disposition des services de police traitant des affaires spécifiques”.

A la Sûreté de l'Etat, on retrouve deux notes de service relatives à la collaboration entre Sûreté de l'Etat et la gendarmerie.

La note du 30 août 1947 insiste sur une collaboration étroite et courtoise, et celle du 22 mai 1956 expose quelles sont les activités spécifiques de la Sûreté de l'Etat et de la gendarmerie dans le domaine de la collecte d'informations (sur le plan de l'ordre public, la gendarmerie est la principale source “ouverte” d'informations pour la Sûreté de l'Etat).

Sur le plan des missions, il existe parfois un chevauchement de compétence entre les services de police et les services de renseignement, à savoir lorsque tous les deux recueillent des informations dans le cadre du maintien de “l'ordre public”.

L'optique des deux services est cependant différente; les services de police, responsables du maintien effectif de l'ordre public, cherchent de préférence des informations immédiatement exploitables, tandis que les services de renseignement sont enclins à rechercher les motivations sous-jacentes et les objectifs cachés.

Si l'information concerne des faits graves sur le point de se commettre, (par exemple un attentat terroriste imminent), le service de renseignement sera naturellement obligé de les transmettre aux autorités compétentes pour exploitation immédiate.

On a récemment constaté que les services de police ont tendance à agir de manière plus "pro-active" (cf. l'article 46 de la Convention d'exécution du Traité de Schengen). Voir aussi plus haut l'interview de l'administrateur général.

En ce qui concerne la note de consensus relative à la répartition des tâches entre services de police, l'administrateur général a déclaré dans son interview qu'il était normal que la Sûreté de l'Etat ne participe pas à ces discussions.

“L'angle d'approche que nous adoptons est tout à fait différent de celui qui entre en ligne de compte dans la note de consensus. Cette dernière parle de la recherche des infractions et se situe donc dans un contexte judiciaire. Ce point ne relève pas des objectifs de la Sûreté de l'Etat et aucune répartition ne s'impose donc en cette matière. Je ne demande d'ailleurs pas l'attribution de compétences policières”.

Plus loin, l'administrateur général met l'accent sur le fait que la Sûreté de l'Etat doit être considérée comme un organe de soutien et non comme une instance concurrente placée à côté ou au-dessus des services de police... *“Je considère que le rôle de la Sûreté de l'Etat vis-à-vis des services de police comme un rôle de soutien et ce, dans un contexte d'interventions judiciaires ou de maintien de l'ordre public. Je suis convaincu- que l'on a absolument besoin d'un service de renseignements, qui ne peut pas être la même chose qu'un service de police. En partant de notre assise de renseignements, nous fournissons un appui sous forme d'informations aux services de police”.*

i.2 Les compétences

Dans l'exécution de leur mission, les agents des services de police disposent de moyens très étendus et légalement définis, notamment en ce qui concerne l'interpellation de personnes.

Puisque la loi ne leur a pas encore donné de compétences clairement définies, les agents des

services de renseignement ne disposent que de moyens très limités pour l'exécution de leurs missions d'information et dépendent en grande partie de la bonne volonté des citoyens.

De fait, ces derniers deviennent "informateurs" des services de renseignement, et leur confiance ne peut pas être trahie, ni leur identité révélée.

Voir l'interview ci-dessus de l'administrateur général: "...A l'inverse, les services de police disposent d'autres sources d'informations efficaces qui ne sont pas directement accessibles à la Sûreté de l'Etat."

i.3 Les directives

Pour les services de police :

La directive du 24 avril 1990 (confidentielle) émanant du Ministre de la Justice et relative aux "*techniques particulières de recherche pour combattre la criminalité grave ou organisée*", modifiée par la circulaire secrète du 5 mars 1992, contient des instructions concernant la gestion des informateurs, valables pour tous les services de police.

Il faut également mentionner la circulaire du 21 novembre 1991 relative à l'utilisation des fonds mis à la disposition des services de police par le Ministère de la Justice.

Le Comité R a étudié ces deux circulaires afin d'examiner dans quelle mesure elles pourraient également s'appliquer aux informateurs des services de renseignement.

Ces directives ont pour but:

- de fixer les règles à suivre par chaque service de police sur la façon d'organiser les contacts avec les informateurs;
- la "*mise au point*" d'un système de contrôle pour s'assurer de la fiabilité des informateurs;
- de prescrire des règles relatives à l'analyse des informations fournies par les informateurs. Cette analyse est basée sur des rapports d'information anonymes et se situe au niveau local, et dans des cas déterminés, au niveau national.

"Ces directives doivent également contribuer à améliorer la coordination de l'intervention des services de police dans la lutte contre la criminalité grave ou organisée, entre autres, dans le domaine du travail avec des indicateurs".

A propos d'un article paru dans "Le Vif - L'Express" et concernant le paiement d'un montant de 8 à 10 millions à un informateur dans l'affaire COOLS, la Sénatrice Madame Milquet, a demandé au ministre de la Justice des explications sur le paiement des informateurs (Sénat - Commission de la Justice - 21 janvier 1997).

Dans sa réponse, le ministre renvoie aux circulaires rappelées ci-dessus. Le ministre ne souhaite ni commenter ni critiquer le système existant. Il a ajouté: "*qu'on prétend que le système a échoué parce qu'un informateur écroulé n'a pas été payé*".

"Il me paraît dès lors évident que nous devons d'abord discuter des aspects éthiques et des limites

du système, avant de prendre des initiatives législatives" dit le ministre.

Il s'est également référé au fait qu'il a chargé un professeur de l'UCL de faire une étude sur le sujet et qu'il a reçu un premier rapport provisoire fin décembre 1996.

"Sur base de ce rapport, je me propose de déposer un projet de loi dans les prochains mois."

Le ministre a encore ajouté que dans son plan d'action contre le crime organisé, le Gouvernement a résolu d'harmoniser les montants des rémunérations versées, avec les systèmes en vigueur dans les pays voisins. La discussion se poursuit en effet non seulement en Belgique, mais également en France et aux Pays-Bas.

"Vu le caractère souvent international du crime organisé, nous devons éviter d'offrir aux informateurs un véritable marché de l'information".

Il est évident qu'on parle ici des informateurs de police.

Dans son interview, l'administrateur général de la Sûreté rappelle que :

" *La différence entre les services de police et les services de renseignement se situent entre autres, sur le plan du mode de rémunération, des éléments de risque et de la durée de la collaboration.*"

" *J'ignore s'il y a eu beaucoup de changements entre-temps, mais jusqu'il y a quelques années, les services de police faisaient souvent appel à des informateurs pour des affaires ponctuelles. A ces occasions, parfois à la suite de la réussite des opérations, des primes étaient payées et ce, en fonction notamment de l'intérêt de l'affaire et des risques qui avaient été pris. La Sûreté de l'Etat recourt davantage à des indemnités fixes. L'approche des services de police présente quelque part des avantages : cela motive les informateurs à bien faire leur travail. D'un autre côté, le recours à des primes occasionnelles peut éventuellement amener l'informateur à provoquer lui-même "des affaires" .*

Ce risque est encore renforcé lorsque l'informateur évolue dans des milieux criminels très lucratifs, où la tentation de jouer sur plusieurs tableaux est parfois grande. Dans la pire des hypothèses, l'informateur peut abuser de son statut en l'utilisant comme couverture pour ses propres activités clandestines illégales, alors qu'il détourne l'attention du service de police avec de "bonnes informations" qui peuvent avoir pour but notamment d'éliminer des criminels concurrents. D'autre part, l'appel aux informateurs par des services de renseignements comporte d'autres risques".

Concernant les services de renseignement

Il n'existe aucune directive ministérielle pour les services de renseignement.

Ceci est sans doute lié au fait que ces services attendent toujours une loi organique.

Certains disposent bien d'ordres et de notes de service internes, mais il n'existe aucune uniformité en la matière entre les différents services.

A la Sûreté de l'Etat

Depuis 1947, 53 ordres de services concernent directement ou indirectement les informateurs.

Au SGR/IH (Humint)

Il n'existe aucune directive écrite, mais des formulaires sont utilisés.

Au SGR/CI (Contre-Ingérence)

Toute la matière concernant les informateurs est réglée par la note de service du 14 février 1995.

6. PROJETS EN COURS D'EXÉCUTION

6.1 Lettres aux Ministres de la Justice et de la Défense nationale

Rappelons qu'en réponse à la question de Madame Milquet sur les informateurs, le ministre de la Justice a déclaré :

" J'ai chargé l'UCL d'une étude sur le sujet et j'ai reçu un premier rapport provisoire fin décembre 1996. Sur base de ce rapport, je me propose de déposer un projet de loi dans les prochains mois." ⁽¹⁾

Cette question concernait clairement les informateurs des services de police.

Le 15 avril 1997, la présidente du Comité R a écrit aux ministres de la Justice et de la Défense nationale afin de leur demander leurs intentions concernant l'élaboration éventuelle d'une législation relative aux informateurs des services de renseignement.

Le ministre de la Justice a répondu le 22 mai 1997 qu'il avait l'intention de rédiger un projet de loi en matière judiciaire. Ses services examinaient depuis plusieurs mois cette problématique en ce qui concerne la Sûreté de l'Etat.

Le ministre a précisé que la Sûreté de l'Etat travaillait d'une manière spécifique avec des informateurs qui faisaient l'objet d'enquêtes de sécurité et d'une rémunération très contrôlée. Les informations livrées ne servant généralement pas en matière judiciaire mais seulement à destination des autorités administratives concernées, la question de la législation se pose avec moins d'acuité en matière de renseignement.

Le ministre informera le Comité R dès qu'il aura défini une position en la matière.

Le ministre de la Défense nationale a, quant à lui, informé le Comité R le 20 juin 1997 que son collègue de la Justice préparait un projet de loi concernant le recours par les services de police aux informateurs et qu'eu égard aux différences importantes qu'il y a entre les missions des services de police et des services de renseignement, il ne lui paraît pas possible d'étendre la réglementation prévue pour les services de police aux services de renseignement. C'est pourquoi il a chargé son Cabinet, en concertation avec le Cabinet du ministre de la Justice d'étudier l'opportunité de préparer ensemble un projet de loi réglant cette matière.

Le ministre a précisé, en outre, qu'à ce stade, il ne lui était pas possible de dire si cette étude conclura à l'opportunité d'une telle réglementation.

⁽¹⁾ Voir plus haut point 3 - (" l'intérêt porté au problème par le Parlement")

6.2. Situation au SGR

Le chef du SGR a fait savoir qu'il s'occupe activement de mettre au point des directives réglant l'utilisation d'informateurs dans les sections IH et CI.

7. CONSTATATIONS

7.1. En général

De toutes les méthodes employées par les services de renseignement pour recueillir des informations secrètes, l'utilisation d'informateurs est la plus fondamentale, mais c'est en même temps la méthode la plus délicate.

En Belgique, cette matière n'est pas réglée par la loi jusqu'à présent. Il n'existe même pas de directives ministérielles applicables aux services de renseignement. Cela est peut-être dû au fait qu'il s'agit d'une matière sensible.

Dans certains services, on retrouve cependant quelques ordres et notes de service internes

Toutefois, l'utilisation d'informateurs pose un certain nombre de problèmes de principe, parmi lesquels :

- les aspects éthiques de l'utilisation d'informateurs (en pratique, on les ignore);
- la protection de la vie privée;
- la problématique de la fiabilité de l'informateur et l'évaluation de l'information;
- le risque de provocation de la part de l'informateur;
- la rémunération des informateurs, dans le contrôle des dépenses et dans le respect de la législation fiscale et sociale;
- la protection des sources; chaque service veille bien sûr à prendre toutes les mesures nécessaires pour protéger l'anonymat de l'informateur. Toutefois, si l'informateur perd son anonymat aucune réglementation n'est prévue pour le protéger physiquement.
- la formation des agents des services et les directives données aux informateurs.

Les différents services ont demandé de légiférer au sujet de leurs missions et de leurs méthodes. L'accès à certaines données a été rendu beaucoup plus difficile depuis l'entrée en vigueur de la loi sur la protection de la vie privée et le traitement des données à caractères personnelles.

Les contacts avec les instances officielles deviennent très délicats et sont entièrement basés sur la "bonne volonté" des personnes approchées, qui devront en conséquence être considérées comme des informateurs.

7.2. A la Sûreté de l'Etat

a) Le Comité R ne peut que déplorer que les réponses de l'administrateur général aient été si

lacunaires dans le cadre de cette enquête de contrôle.

L'administrateur général n'a fourni aucun éclaircissement sur les risques liés à l'utilisation d'informateurs par les services de renseignement.

Dans l'interview accordée à "Politeia", il a par contre explicitement fait référence au fait que l'utilisation d'informateurs entraîne pour les services de renseignement d'autres risques que pour les services de police. Il ne s'est pas étendu davantage sur ce sujet.

Il a aussi prétendu que le traitement des informateurs était stratégiquement mieux développé à la Sûreté de l'Etat que celui en vigueur dans les services de police. ⁽¹⁾

- b) Selon les informations fournies par ce service de renseignement, le travail avec des informateurs pose peu de problèmes.
- c) Depuis 1947, 53 ordres et notes de service concernant directement ou indirectement les informateurs ont été rédigés. Théoriquement, tous les ordres et notes de service qui n'ont pas été annulés restent d'application.

Il existe peu de directives qui concernent la façon dont l'agent doit utiliser ses informateurs et la manière dont l'agent doit traiter l'information dans son rapport.

Plus du tiers des ordres et notes de service concernent l'emploi des fonds.

- d) La Sûreté de l'Etat a organisé en son sein un groupe de travail chargé de revoir de manière approfondie les ordres et notes de service.
- e) Ce groupe de travail élabore également une proposition pour une meilleure protection extérieure des sources, sur base légale.
Après l'informatisation, des mesures seront également prises pour la protection de l'anonymat des informateurs au sein même de la Sûreté de l'Etat.
- f) Par lettre du 22 mai 1997, le ministre de la Justice a fait savoir au Comité R qu'il réfléchit à une législation qui préciserait l'utilisation des informateurs dans des affaires judiciaires.
En ce qui concerne les services de renseignement, le ministre estime qu'une législation en la matière n'est pas urgente.
- g) Suivant l'administrateur général, l'infiltration effectuée par des agents du service qu'il dirige n'est pas autorisée.
- h) Suivant un responsable de la Sûreté de l'Etat, deux agents au moins devraient encadrer un informateur, dont l'un serait toujours spécialisé dans le domaine de l'information recherchée.
Suivant le Service d'enquêtes du Comité R, les sections ont tenté d'atteindre cet objectif. Une telle situation correspondrait à l'idéal.
- i) Durant leur période de stage, les inspecteurs devaient suivre un cours sur le recrutement et la manière d'approcher les informateurs. Les cours étaient donnés par des membres expérimentés de la Sûreté de l'Etat. Ils n'ont pas eu d'autre formation.
D'après l'expérience du Service d'enquêtes du Comité R, il s'agissait de cours obsolètes et les dernières promotions n'auraient plus reçu de formation à ce sujet.
Il n'y a pas eu de nouveaux recrutements ces dernières années et à l'avenir de nouveaux cours seront nécessaires.

⁽¹⁾ op cit.

7.3. AU SGR

7.3.1. En général

Le ministre de la Défense nationale a chargé son Cabinet d'examiner, en concertation avec le Cabinet du ministre de la Justice, l'opportunité de préparer ensemble un projet de loi réglant cette matière. En outre, le ministre a précisé qu'à ce stade, il ne lui était pas possible de dire si cette étude va conclure à l'opportunité d'une telle réglementation.

7.3.2 Au SGR/IH

- a) Il n'existe pas de directives écrites.
- b) D'après le responsable de cette section au SGR, l'utilisation d'informateurs pose peu de problèmes. Toutefois, cette section reste continuellement vigilante afin d'éviter toute infiltration par des services de renseignement étrangers ou d'être victime de désinformation.
- c) Les membres du personnel ne bénéficient pas de formation spécifique. Ils suivent parfois un cours à l'étranger. Le personnel provient d'unités différentes. La carrière des personnes employées dans cette section est généralement de courte durée.

7.3.3. Au SGR/CI

- a) Depuis le 14 février 1995, il existe une note de service qui traite de manière globale la matière des informateurs en ce y compris leur rémunération. Actuellement, elle fait l'objet d'un réexamen surtout en ce qui concerne la procédure d'évaluation de l'informateur.
- b) Une liste des sources administratives que le service doit obligatoirement pouvoir consulter sans faire appel à la "bonne volonté" d'autres personnes a été établie.
- c) L'informateur n'est pas autorisé à collaborer en même temps pour un service étranger; cependant il peut aussi être en relation avec la Sûreté de l'Etat.
- d) Si les informateurs n'ont pas un rendement suffisant, ils sont remerciés. Le service est conscient que l'informateur, lorsqu'il est mis fin à la collaboration, sera tenté de vouloir lui porter préjudice et il en est tenu compte.
- e) Tout le personnel de cette section suit une formation à l'Ecole Royale Militaire. Certains membres du personnel reçoivent une formation à l'étranger, notamment aux Pays-Bas, en France et en Allemagne.

8. RECOMMANDATIONS

- a) La distinction entre l'information reçue des administrations et celle provenant de "véritables informateurs" doit faire l'objet d'une loi claire.

Le Comité R a pris connaissance du projet de loi portant réglementation des services de renseignement et de sécurité, qui stipule notamment en son article 10 que les magistrats de l'ordre judiciaire et les fonctionnaires et agents des services publics peuvent fournir les

informations demandées par les services de renseignement, en tenant compte de la loi et des modalités déterminées par leurs autorités hiérarchiques

Le projet prévoit également que l'accès aux registres de la population et aux registres des étrangers sera réglé par arrêté royal.

Il paraît évident que les services publics doivent respecter la loi quand ils fournissent ces renseignements, mais le Comité R s'interroge sur les modalités d'application de cette disposition qui doit être fixée par les responsables hiérarchiques. Ne peut-on craindre là une possibilité d'arbitraire ?

La loi néerlandaise prévoit que les services peuvent s'adresser à d'autres organes publics pour recueillir les données nécessaires à la bonne exécution de leurs missions. Toutefois, les travaux préparatoires, insistent sur le fait que cette compétence ne peut déroger à l'application d'autres dispositions législatives relatives aux données demandées. En outre, il existe aux Pays-Bas une réglementation particulière relative à l'obtention de données judiciaires. La législation néerlandaise semble être plus explicite en la matière que le projet de loi belge.

Le Comité recommande que le projet de loi en la matière soit adapté par analogie avec la législation néerlandaise.

- b) La problématique de la collaboration, aussi bien des services belges de renseignement entre eux qu'avec les autorités judiciaires, les services de police et les services étrangers de renseignement, n'est traitée que de façon très succincte par le projet de loi.

La collaboration et la coordination entre les services de renseignement semblent évoluer dans un sens favorable, en particulier depuis la conclusion du protocole d'accord entre le SGR et la Sûreté de l'Etat.

Selon l'administrateur général, les contacts entre la Sûreté de l'Etat et la gendarmerie, surtout avec le Bureau Central de Recherches, sont bons.

Lors de la réunion qui a eu lieu au Comité R le 26 mai 1997, dans le cadre de l'examen de l'accord évoqué ci-dessus, l'administrateur général a parlé en termes positifs d'une étroite collaboration avec les différents services de police permettant d'arriver à un réel échange d'informations.

Seule une véritable collaboration entre les différents services permettra d'éviter la perte ou le manque de circulation de l'information.

Le Comité R recommande de développer cette collaboration à l'avenir.

- c) On peut discuter à l'infini sur le bien fondé d'une loi réglant l'utilisation d'informateurs.

Le Comité R, quant à lui, recommande qu'une loi soit édictée et qu'elle fixe les principes suivants:

- le recours à l'informateur ne peut s'envisager que lorsque l'exploitation des autres sources (sources ouvertes) est inopérante.
(principe de subsidiarité);
- la loi devra prévoir qu'il convient de faire la balance des intérêts entre l'utilisation d'un informateur et le préjudice qui pourrait en résulter pour les particuliers dans la violation de leurs droits individuels.
(principe de proportionnalité);

- la loi devra fixer les délits devant obligatoirement être dénoncés par l'informateur et les cas où l'informateur ne sera pas soumis à cette obligation dans l'intérêt de l'opération menée par le service de renseignement (en analogie avec la législation allemande - Strafprozessordnung § 138).
- **la protection externe de l'informateur, en ce compris, sa protection physique.** En cas de danger imminent pour la vie ou l'intégrité physique d'un informateur, il faudrait prévoir la possibilité de lui fournir (par analogie à la réglementation américaine) une autre identité.

d) Le Comité R recommande de régler les autres aspects de l'utilisation des informateurs par des directives précises.

De telles directives existent en Belgique pour les services de police. Dans d'autres pays, elles existent aussi pour les services de renseignement, par exemple au Canada, le CSIS (Canadian Security Intelligence Service) Act guidelines; aux U..A. le FBI guidelines et au Royaume Uni "the Security Service" ont leurs propres directives concernant le recrutement et la gestion des informateurs. Ces directives prévoient à la fois le contrôle des informateurs et celui des agents des services de renseignement. Elles n'ont cependant pas force de loi.

Les directives belges devraient stipuler :

d.1 Code de conduite pour l'informateur

Les agents portent à la connaissance des informateurs que leur collaboration se fait sur base des règles suivantes :

- interdiction d'être impliqué dans des activités illégales. Comme prévu dans les directives de la police belge et dans celles du FBI, il ne pourra y être dérogé que dans des circonstances exceptionnelles, telles que
 - si l'information est d'importance capitale et ne peut raisonnablement être obtenue d'une autre manière;
 - s'il n'existe pas d'autres moyens de préserver la couverture et l'anonymat de l'informateur;
 - en cas de menace contre la vie et l'intégrité physique des particuliers.

Chaque exception fait l'objet d'une autorisation écrite du chef du service, excepté en cas d'extrême urgence. Dans ce dernier cas, un rapport immédiat et motivé est adressé au chef du service.

Le Comité R est conscient qu'aucune législation n'autorise des pratiques illégales ou criminelles. C'est pourquoi ces exceptions doivent être appliquées avec la plus grande circonspection et faire l'objet d'un contrôle sévère.

- veiller à ne pas jeter le discrédit sur le service;
- les informateurs ne peuvent en aucun cas agir comme agents provocateurs.

d.2 Comportement des agents des services de renseignement et élaboration de rapports

Les membres des services de renseignement doivent recevoir des instructions sur la façon de

traiter les informateurs.

Les principes suivants qui doivent être respectés sont déjà partiellement appliqués dans la pratique:

- dans chaque service ou section, un "gestionnaire des informateurs" est désigné (cette tâche pourrait être assurée par le chef de brigade ou de section), responsable de la manière dont les contacts avec les informateurs sont entretenus et sur la façon dont les rapports sont rédigés. Ce gestionnaire des informateurs a aussi pour tâche de suivre les agents des services et de veiller à leur intégrité.
- les contacts avec un informateur sont toujours assurés par deux agents, afin d'éviter tout risque de manipulation de l'agent par l'informateur.
- chaque information émanant d'un informateur fait l'objet d'un rapport.
- l'informateur reçoit, dans la mesure du possible, des instructions précises et les agents vérifient s'il les respecte.

d.3 Règles relatives à l'évaluation des informateurs

Dès le début de l'enquête parlementaire sur l'organisation de la lutte contre le banditisme et le terrorisme, des questions ont été posées sur l'évaluation de la fiabilité d'un informateur et l'appréciation de l'information par les analystes. ⁽¹⁾

Le Comité R est conscient que, la promulgation d'un règlement en cette matière rencontre des objections. Il estime toutefois qu'il faut essayer de déterminer de manière cohérente certains critères d'évaluation des informateurs des différents services de renseignement. Nul ne contestera que les informateurs sont d'un intérêt capital pour les services de renseignement, mais cela implique aussi d'accorder le plus grand soin à leur fiabilité et à leur évaluation.

Le Comité R recommande que l'évaluation soit par exemple réalisée par une équipe indépendante et expérimentée du service de renseignement concerné.

Cette équipe serait également chargée de la mise à jour et de la proposition de directives en cette matière, en ce compris celles qui ont trait à la formation des agents.

d.4 Contrôle des informateurs

Le fait de désigner un gestionnaire des informateurs, le fait que les contacts avec l'informateur soient toujours pris par deux agents et l'existence d'une équipe, chargée notamment de l'évaluation des informateurs constituent déjà un contrôle certain.

Il est de plus indiqué d'établir, comme dans les services de police, **une codification commune des informateurs pour les deux services de renseignement.**

⁽¹⁾ Voir point 3 de l'intérêt parlementaire pour le problème.

L'identité des informateurs doit être encodée afin de sauvegarder leur anonymat. D'autre part, cette codification permettrait de vérifier si un informateur est déjà connu d'un autre service de renseignement et s'il est éventuellement signalé comme "inactif " ou "non fiable".

Enfin, ce système permettrait un contrôle supplémentaire de l'informateur et pourrait faire l'objet d'un addendum au protocole d'accord conclu entre la Sûreté de l'Etat et le SGR.

d.5 Paiement des informateurs

Le Comité R est d'avis que cet aspect du sujet de l'enquête doit faire l'objet d'une réglementation pour les services de police comme pour les services de renseignement. Cette réglementation doit porter sur :

- l'usage des fonds;
- le contrôle interne et externe du paiement des informateurs;
- la rédaction d'un rapport annuel sur l'usage des fonds,

Cela permettrait au Comité R d'exercer un contrôle plus efficace.

En vue de la protection de l'informateur, l'identité des bénéficiaires des paiements ne figurera pas dans la comptabilité. Il sera fait usage du code d'identification.

Le mode de paiement doit être réglé de manière à permettre non seulement un contrôle réel mais aussi à garantir l'anonymat de l'informateur.

Il faut tendre à la plus grande uniformité possible dans le paiement des indemnités en prévoyant une tarification des rémunérations.

e) Le Comité R recommande, par analogie avec certains autres pays, une formation appropriée des agents des services extérieurs et des analystes.

Une formation commune pourrait être dispensée dans notre propre pays aux membres de la Sûreté de l'Etat et à ceux du SGR. ⁽¹⁾

9. CONCLUSION GÉNÉRALE

Le Comité R souhaite insister à nouveau sur le caractère théorique de cette enquête, qui a pour but d'identifier les problèmes qui peuvent se poser à l'occasion de l'utilisation d'informateurs, et d'en dégager des premières recommandations.

Le Comité R continuera à traiter cette matière à l'avenir, mais sous forme de "case study" en se conformant aux règles de confidentialité requises en la matière.

Depuis les récents événements dramatiques survenus en Belgique, le problème des informateurs

⁽¹⁾ Voir aussi l'étude de la législation néerlandaise sur les services de renseignement et de sûreté - tome IV - point 10 - la formation et l'instruction des fonctionnaires des services de renseignement et de sûreté.

de police a souvent été évoqué. La matière mérite cependant d'être traitée en ce qui concerne les informateurs des services de renseignement. La collaboration entre services de police et services de renseignement à l'occasion des sujets comme la criminalité organisée, le terrorisme, etc... devra faire l'objet d'une attention particulière.

Le risque existe, en effet, que dans les domaines mentionnés ci-dessus, la différence entre informateur des services de police et de renseignement s'estompe et que les deux services devront face à des problèmes comparables.

Par lettre du 14 juillet 1997, le chef du SGR a transmis ses remarques concernant la présente enquête de contrôle. Compte tenu de ces remarques, le Comité R est d'avis qu'il serait souhaitable d'organiser un échange de vues avec les services concernés.

Conformément à l'article 33 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement, il a été proposé aux ministres compétents d'organiser cet échange de vues.

Le 1^{er} septembre 1997, le Ministre de la Justice a adressé au Comité R la lettre suivante :

“Je vous informe que la Sûreté de l'Etat elle-même a constitué un groupe de travail de manière à examiner la problématique des informateurs en son sein et les travaux seront bientôt terminés. Ceux-ci vous seront dès lors communiqués en vue de procéder à des échanges de vues sur cette importante question.

Pour le reste, je n'ai pas de remarques particulières à formuler à l'égard de votre rapport.”

CHAPITRE 2 : STATUTS DES MEMBRES DES SERVICES DE RENSEIGNEMENT

SECTION 1 : LES STATUTS DES MEMBRES DU PERSONNEL DU SGR

L'ouverture de cette enquête a été décidée par le Comité lors de sa réunion tenue le 24 novembre 1995.

Le rapport général d'activités que le Comité a présenté à la Chambre des représentants et au Sénat le premier jour de leur session ordinaire d'octobre 1996 comprenait un premier rapport concernant les statuts des membres de la Sûreté de l'Etat. Au cours de la session parlementaire 1996-1997, le Comité R a poursuivi son enquête sur les statuts des membres du Service Général du Renseignement et de la Sécurité.

Le présent chapitre constitue le rapport sur ce second volet de l'enquête. Celle-ci s'intéresse aussi à la situation des agents des services de renseignement en temps de guerre ainsi qu'à leur statut syndical.

On trouve au SGR du personnel, civil et militaire, soumis à différents statuts. On y trouve également du personnel détaché de la gendarmerie. Les statuts des membres de ce personnel sont fixés par plusieurs lois, arrêtés royaux et arrêtés ministériels.

Le projet de loi organique des services de renseignement et de sécurité, déposé à la Chambre des représentants par le gouvernement le 2 juillet 1996, contient des dispositions relatives au personnel des services de renseignement. Le législateur s'intéresse donc aux statuts des membres du personnel de ces services. Ces statuts participent sans aucun doute à l'efficacité de ces services que le Comité R est légalement chargé de garantir.

La section Sécurité du SGR est notamment composée d'agents civils dotés d'un statut quasi identique à celui des agents des services extérieurs de la Sûreté de l'Etat. Ce statut des agents civils du SGR/S a donc été examiné en le comparant au statut des agents de l'Etat (arrêté royal

du 2 octobre 1937) et à celui des agents des services extérieurs de la Sûreté de l'Etat (arrêté royal du 29 avril 1966 portant le statut du personnel de la section Sûreté de l'Etat de l'Administration de la Sûreté publique).

Un volumineux chapitre est consacré à ces différents statuts. Pour des raisons pratiques, il a été décidé de publier cette étude complète sous forme d'un tiré à part en annexe du rapport d'activités de 1997.

SECTION 2 : LES AGENTS CONTRACTUELS DE LA SÛRETÉ DE L'ETAT

1. POURSUITE DE L'ENQUÊTE - PROCÉDURE

Le rapport d'activités de 1996 mentionnait dans son chapitre 5, point 2.5. qu'une enquête se poursuivait afin de vérifier sur quelle base légale et réglementaire dix agents contractuels ont été mis au travail dans les services administratifs de la Sûreté de l'Etat.

L'enquête s'est donc poursuivie. Un rapport provisoire a été adressé au ministre de la Justice le 20 novembre 1996 avec demande d'organiser un échange de vues sur la question conformément à l'article 33, alinéa 5 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

Le présent rapport a été approuvé par le Comité R le 26 juin 1997. Il a été adressé au ministre de la Justice le 27 juin 1997.

2. L'INTÉRÊT PARLEMENTAIRE POUR LE PROBLÈME

Une question parlementaire a été posée le 3 septembre 1996 par le député Jan Eeman (VLD) au ministre de la Justice ⁽¹⁾. La question portait notamment sur le nombre et le pourcentage des agents contractuels du ministère de la Justice par rapport à l'ensemble de son personnel. La réponse du ministre donne quelques chiffres intéressants ainsi que des informations utiles dans le cadre de la présente enquête. Ces données seront exposées dans le rapport qui suit.

3. EXPOSÉ DE LA SITUATION

La situation des agents contractuels de la Sûreté de l'Etat doit être examinée en tenant compte de l'effectif global de ces agents au ministère de la Justice. Les données du ministère de la Fonction publique indiquent que le ministère de la Justice emploie 1.107 agents contractuels, soit environ 15% de ses effectifs. Le ministre de la Justice a précisé que l'administration centrale (au sein de laquelle se trouvent les services administratifs de la Sûreté de l'Etat) occupait 253 contractuels ⁽²⁾.

Le ministre n'indique pas combien parmi ces agents contractuels sont occupés dans les services administratifs de la Sûreté de l'Etat. A propos des services extérieurs de ce service, le ministre indique cependant qu'un agent contractuel est employé à temps plein pour le remplacement de membres du personnel bénéficiant de la semaine volontaire de quatre jours.

Par sa lettre du 19 mai 1994, l'administrateur général de la Sûreté de l'Etat avait informé le Comité R que le cadre de ses services d'analyse et administratifs était incomplet. En vue de faire face à un accroissement évident du travail dans ces services, l'administrateur général a demandé le 21 avril 1994 au ministre de la Justice de pouvoir disposer très rapidement d'agents

⁽¹⁾ Chambre des représentants - session ordinaire de 1996/1997 - questions et réponses n°. 81 - 12 mai 1997 - p. 11.112 et suivante

⁽²⁾ Idem.

contractuels.

Selon la note de restructuration entrée en vigueur le 1^{er} avril 1996, dix agents contractuels étaient employés à la Sûreté de l'Etat. Ce chiffre fut confirmé par l'administrateur général dans sa lettre adressée au Comité R le 12 juillet 1996. Le Service d'enquêtes du Comité R a examiné les dossiers administratifs de ces dix agents.

Par sa lettre du 12 juillet 1996, l'administrateur général a également expliqué que le cadre organique fixé par l'arrêté royal du 6 avril 1995 pour le personnel de l'administration centrale du ministère de la Justice et, donc de la Sûreté de l'Etat, était en déficit de 20 personnes. Les renforts souhaités concernaient particulièrement des analystes dont la Sûreté de l'Etat avait un besoin prioritaire.

La note de service du 20 septembre 1996 modifiant partiellement les structures des services administratifs et communs de la Sûreté de l'Etat a fait apparaître que seize nouveaux agents contractuels y ont été affectés. Ceci portait à 26 le nombre d'agents contractuels en service à la Sûreté de l'Etat (soit environ 20% de son cadre administratif). Ceux-ci se répartissaient comme suit :

- niveau 1 : trois conseillers adjoints et un expert;
- niveau 2 : une secrétaire de direction et trois assistants administratifs;
- niveau 3 : quatre commis;
- niveau 4 : quatre ouvriers et dix nettoyeuses.

S'agissant de personnes affectées à des tâches logistiques et d'entretien non spécifiques à un service de renseignement, le Comité R ne s'est pas estimé utile de se pencher davantage sur la situation des agents contractuels du niveau 4.

4. LES PRINCIPES LÉGAUX APPLICABLES

Les principes fondamentaux en matière de recrutement de personnel par les services de l'Etat sont fixés par la loi du 22 juillet 1993 portant certaines mesures en matière de fonction publique. Cette loi a remplacé l'arrêté royal n° 56 du 16 juillet 1982 relatif au recrutement dans certains services publics. Ces services publics ne peuvent recruter des agents statutaires que dans les limites de leur enveloppe de recrutement (article 1^{er} de la loi du 22 juillet 1993).

En principe, la situation du personnel des administrations et autres services de l'Etat fédéral est statutaire : *“Nonobstant toute autre disposition, les recrutements sont effectués exclusivement selon les règles permanentes prévues dans les statuts du personnel”* (article 3, § 1^{er} de la loi du 22 juillet 1993).

L'article 4, § 1^{er} de cette loi détermine cependant que *“par dérogation à l'article 3, dans les administrations et autres services des ministères fédéraux (...), il peut être procédé à l'engagement de personnes sous le régime du contrat de travail aux fins exclusives :*

- 1° *de répondre à des besoins exceptionnels et temporaires en personnel, qu'il s'agisse soit de la mise en oeuvre d'actions limitées dans les temps, soit d'un surcroît extraordinaire de travail;*
- 2° *de remplacer des agents qui n'assument pas leur fonction ou ne l'assument qu'à temps partiel, et ce sans préjudice de la possibilité de remplacer un agent statuaire par un autre agent statuaire;*

3° d'accomplir de tâches auxiliaires ou spécifiques.

§ 2. Après négociation avec les organisations syndicales représentatives et sur proposition du Ministre qui a la fonction publique dans ses attributions, le Roi détermine :

1° les conditions et les modalités de l'engagement des personnes sous contrat de travail (...) et ce, dans le respect de la loi du 3 juillet 1978 relative aux contrats de travail;

2° les tâches auxiliaires ou spécifiques visées au § 1^{er}, 3°."

Un arrêté royal est aussi nécessaire afin de fixer par niveau le nombre de personnes qui peuvent être engagées sous contrat de travail en vue de répondre aux besoins exceptionnels et temporaires en personnel visés à l'article 4 § 1^{er}, 1° précité. Cet arrêté royal détermine la durée de leur occupation. Si la durée d'occupation est supérieure à six mois, l'arrêté royal en question doit être délibéré en Conseil des Ministres (article 4, §4 de la loi du 22 juillet 1993).

Aucun arrêté royal complémentaire n'est nécessaire pour procéder à l'engagement d'agents contractuels en vue de remplacer des agents qui n'assument pas leur fonction ou ne l'assument qu'à temps partiel (ceci, en application de l'article 4, §1^{er}, 2°).

La loi du 22 juillet 1993 a aussi prévu un système pour contrôler la régularité de tout acte de recrutement ou de mise au travail sous contrat de travail dans un service de l'Etat.

5. LES ARRÊTÉS ROYAUX D'APPLICATION

L'arrêté royal du 18 novembre 1991 avait déjà fixé les conditions d'engagement par contrat de travail dans les administrations de l'Etat et autres services des ministères. Cet arrêté royal est toujours en vigueur; il est d'application aux agents contractuels de la Sûreté de l'Etat.

Pour être engagé par contrat de travail dans l'administration, il faut répondre à la plupart des conditions d'admissibilité prévues par le statut des agents de l'Etat (article 16 de l'arrêté royal du 2 octobre 1937), être belge pour les fonctions qui impliquent une participation effective à l'exercice de la puissance publique, être porteur des mêmes diplômes et certificats d'étude que ceux requis pour être nommé. En outre, pour les fonctions contractuelles des niveaux 1, 2 et 3, les candidats doivent être soit déjà en service ou mis au travail dans l'administration, soit lauréats d'un concours de recrutement, d'un examen de capacité ou d'un test de sélection organisé par le Secrétariat permanent de recrutement.

A la Sûreté de l'Etat, la candidature des agents contractuels doit en plus, tout comme celle des agents statutaires d'ailleurs, être agréée par le ministre de la Justice, conformément à l'article 33 de l'arrêté royal du 29 avril 1966 portant le statut du personnel de la Sûreté de l'Etat. Aucune disposition n'indique si ces agents doivent disposer ou non d'un certificat de sécurité.

Un arrêté royal du 1^{er} février 1993, pris en exécution de l'arrêté royal n° 56 du 16 juillet 1982 relatif au recrutement dans certains services publics détermine les tâches auxiliaires ou spécifiques pour lesquelles il peut être procédé à l'engagement de personnes sous contrat de travail. Cet arrêté royal est resté en vigueur pour l'application de la loi du 22 juillet 1993 (article 34 de la loi).

L'article 1^{er} de cet arrêté royal définit notamment comme tâches auxiliaires ou spécifiques, "les

tâches qui peuvent être confiées : (20°) à des experts pour exercer des tâches correspondant à des fonctions de niveau 1 et qui exigent une qualification requise pour une durée limitée ou pour une activité nettement définie”.

Un “expert” est au moins titulaire d’un diplôme donnant accès aux emplois de niveau 1 et doit répondre aux qualifications professionnelles particulières précisées dans une analyse de fonction. Le contrat de travail définit les tâches confiées à l’expert ainsi que la qualification professionnelle requise pour une durée limitée ou pour une activité nettement définie (article 2, alinéa 3).

Ces membres du personnel *“peuvent être engagés en vertu d’un contrat de travail conclu à temps plein ou à temps partiel sur autorisation de l’inspecteur des Finances ou sur autorisation préalable du commissaire du gouvernement désigné sur proposition du Ministre des Finances ou du délégué du Ministre des Finances”*(article 1^{er}, alinéa 2).

6. LES FONDEMENTS DE L’ENGAGEMENT D’AGENTS CONTRACTUELS À LA SÛRETÉ DE L’ETAT

L’arrêté royal du 20 décembre 1995 a autorisé l’administration de la Sûreté de l’Etat à recruter deux conseillers adjoints et quatre assistants administratifs en vue aussi de *“répondre à des besoins exceptionnels et temporaires en personnel”,* à savoir *“effectuer le tri et la suppression de documentation”*(voir rapport d’enquête sur la destruction des dossiers).

Dans sa lettre du 12 juillet 1996, l’administrateur général de la Sûreté de l’Etat ne mentionnait aucun autre arrêté royal permettant à son service de recruter du personnel contractuel. Il indiquait alors que les recrutements autorisés par l’arrêté royal du 20 décembre 1995 étaient en cours.

Selon le secrétaire général du ministère de la Justice (lettre du 30 septembre 1996), sept des personnes précitées *“ont été engagées en vertu des dispositions de l’article 4 de la loi du 22 juillet 1993 portant certaines mesures en matière de fonction publique, qui permet de procéder à l’engagement de personnel contractuel en vue de remplacer des agents qui n’assument pas leur fonction ou ne l’assument qu’à temps partiel (par exemple, en cas de pause-carrière, détachement dans un cabinet ministériel, prestations réduites)”*. S’agissant du motif d’engagement repris par l’article 4 §1er, 2° de la loi précitée, aucun arrêté royal complémentaire n’est nécessaire pour déterminer le nombre de personnes qui peuvent être occupées pour répondre à ce besoin.

Enfin le secrétaire général explique l’engagement de trois autres personnes par la seule mention de la loi du 3 juillet 1978 relative aux contrats de travail comme base de leur engagement, ce qui n’est pas une justification suffisante en regard de l’article 4 de la loi du 22 juillet 1993.

Selon le ministre de la Justice, l’engagement d’un expert reposait sur l’article 1^{er}, 20° de l’arrêté royal du 1^{er} février 1993 *“déterminant les tâches auxiliaires ou spécifiques dans les administrations et autres services des ministères ainsi que dans certains organismes d’intérêt public”*(lettre du 12 mars 1997).

“Tous ces contrats ont été visés favorablement par l’inspecteur des finances attaché au département” (lettre du 30 septembre 1996 du secrétaire général du ministère de la Justice).

Enfin, selon l’administrateur général de la Sûreté de l’Etat (sa lettre du 12 juillet 1996), la candidature de tous les agents contractuels de la Sûreté de l’Etat est agréée par le ministre; ceux-ci font l’objet d’une enquête de sécurité approfondie.

7. LES VÉRIFICATIONS ET CONSTATATIONS DU SERVICE D'ENQUÊTES

Trois apostilles ont été adressées au Service d'enquêtes les 30 juillet 1996, 2 septembre 1996 et 27 mars 1997. Les missions confiées consistaient à vérifier les dossiers administratifs de certains agents contractuels des niveaux 1 et 2 en fonction à la Sûreté de l'Etat.

Les constatations du Service d'enquêtes peuvent être résumées comme suit :

- Au moment des vérifications, seuls deux conseillers adjoints et un assistant administratif avaient été recrutés en application de l'arrêté royal du 20 décembre 1995 en vue "*d'effectuer le tri et la suppression de documentation*". Toutefois, les deux conseillers adjoints étaient occupés à d'autres tâches que "*le tri et la suppression de documentation*" : l'un était affecté au service juridique et était investi de la qualité de "porte parole" de la Sûreté de l'Etat, l'autre était affecté à l'exploitation du réseau Internet au service de documentation générale. Seul l'assistant administratif était spécifiquement affecté au tri et à la suppression de dossiers. Ces constatations résultent également de la note de service du 20 septembre 1996.
- L'expert-analyste paraissait satisfaire aux conditions d'engagement requises par l'article 1, 20° de l'arrêté royal du 1^{er} février 1993 pour le recrutement d'experts dans certains services publics sous contrat de travail. Toutefois, son dossier ne comportait aucune analyse de fonction précisant les qualifications professionnelles requises de la part de l'intéressé. Son contrat ne définissait pas non plus les tâches qui lui étaient confiées ni sa qualification professionnelle. Une note de l'administrateur général attestait par contre que la personne répondait aux conditions requises sur le plan de la spécialisation dans une matière déterminée.
- Deux cas mis à part (notamment celui de l'expert-analyste), les dossiers administratifs consultés ne contenaient aucune trace écrite de l'avis que doit donner l'administrateur général de la Sûreté de l'Etat au ministre de la Justice en vue de l'agrément préalable des candidatures telle que prévue par l'article 33 de l'arrêté royal du 29 avril 1966 portant le statut du personnel de la Sûreté de l'Etat.
- Les agents contractuels de la Sûreté de l'Etat ont effectivement fait l'objet d'une enquête de sécurité. Ces enquêtes ont cependant été effectuées après l'entrée en service des intéressés, ce qui est contraire aux règles de sécurité en la matière. Le Service d'enquêtes estime par ailleurs que dans le cas de l'expert-analyste, la Sûreté de l'Etat n'a pas eu la possibilité d'effectuer l'enquête de sécurité appropriée au niveau requis par les fonctions de l'intéressée.
- Les contractuels recrutés "*en vue de remplacer des agents qui n'assument pas leur fonction ou ne l'assument qu'à temps partiel*" n'étaient pas toujours affectés aux mêmes tâches que ces derniers assumaient avant leur départ. Ainsi par exemple, la personne engagée pour compenser les heures de travail non prestées par des inspecteurs des services extérieurs travaillant à temps partiel était affectée comme secrétaire de direction dans un service d'étude; celle-ci restait toutefois à charge du budget des services extérieurs. De même, une secrétaire d'administration engagée en remplacement d'un membre de la Sécurité nucléaire était également affectée dans un service d'étude de la Sûreté de l'Etat.

8. CONCLUSIONS

Au cours de ces dernières années, le Gouvernement a pris des mesures visant toute la Fonction

publique fédérale :

- blocage des recrutements, même pour remplacer des départs définitifs;
- établissement de nouveaux cadres coïncidant avec les effectifs réduits existant;
- possibilités de travail à temps partiel ou d'interruption de carrière.

A ces mesures, il faut ajouter les nombreuses possibilités de congés et de détachement déjà applicables.

Dans ce contexte, le cadre des agents de la Sûreté de l'Etat n'est pas complet. Ce service cherche dès lors à pallier aux insuffisances en procédant au recrutement d'agents contractuels. Ce personnel représente environ 20% du cadre administratif, ce qui est une proportion anormalement élevée.

Dans l'état actuel de la législation (la loi du 22 juillet 1993 et ses arrêtés d'application), l'engagement des agents contractuels de la Sûreté de l'Etat trouve ainsi son fondement légal:

- dans un arrêté royal du 20 décembre 1995 qui permet l'engagement de six personnes pour *"répondre à des besoins exceptionnels et temporaires en personnel"*;
- dans l'article 1^{er}, 20° de l'arrêté royal du 1^{er} février 1993 qui permet l'engagement d'experts (jusqu'à présent, une personne est concernée);
- dans l'article 4 de la loi du 22 juillet 1993 qui permet de procéder à l'engagement de personnel contractuel en vue de remplacer des agents qui n'assument pas leur fonction ou ne l'assument qu'à temps partiel (pause-carrière, prestations réduites, congés divers, etc ... : une vingtaine de personnes sont concernées).

Cependant les motifs invoqués par l'administrateur général pour demander l'engagement d'agents contractuels (à savoir le cadre incomplet de son service et l'accroissement évident du travail) ne correspondent pas à un des motifs admis par l'article 4 §1^{er} de la loi du 22 juillet 1993. Le problème du déficit permanent du cadre administratif, aggravé par l'accroissement du travail, doit trouver sa solution dans l'engagement d'agents statutaires.

Les vérifications effectuées sur place montrent que les agents recrutés dans les liens d'un contrat d'emploi ne sont pas toujours affectés aux tâches des personnes qu'ils sont censés remplacer ou bien aux tâches spécifiques pour lesquelles ils sont censés être engagés. Ceci résulte du fait que certaines de ces tâches administratives spécifiques (par exemple, le tri des dossiers) peuvent difficilement être confiées à des personnes engagées à court terme sans aucune expérience préalable dans les services de renseignements.

De plus, il apparaît que la personne engagée pour remplacer plusieurs agents des services extérieurs travaillant à temps partiel est affectée dans un service administratif. Le transfert d'heures de travail ici opéré au profit des services administratifs au détriment des services extérieurs se justifie ici aussi par la spécificité de leurs missions. Toutefois, cette situation ne paraît pas conforme au principe de la "barrière" instaurée entre les services extérieurs de la Sûreté de l'Etat et les autres services des administrations de l'Etat (article 3 de l'arrêté royal du 29 avril 1966 portant le statut du personnel de la section Sûreté de l'Etat de l'Administration de la Sûreté publique).

Dans l'étude consacrée au statut des agents civils du Service de sécurité militaire (voir annexe au rapport d'activités 1997), le Comité R met sérieusement en doute la pertinence de cette barrière. La situation ici décrite est un argument supplémentaire qui plaide en faveur de la suppression de celle-ci.

En résumé, plutôt que d'avoir à recourir à toutes sortes de "ficelles" administratives et statutaires, le Comité R estime que la Sûreté de l'Etat devrait pouvoir procéder au recrutement de personnel statutaire pour remplir son cadre légal.

Par ailleurs, les agents contractuels de la Sûreté de l'Etat n'ont fait l'objet d'une enquête de sécurité que postérieurement à leur engagement, ce qui est contraire aux règles de sécurité habituellement appliquées en la matière. Une des enquêtes n'a pu être menée au niveau requis par les fonctions exercées par l'agent.

9. RECOMMANDATIONS

Le Comité R insiste de nouveau pour qu'il soit pourvu de manière effective aux cadres organiques de la Sûreté de l'Etat par le recrutement d'agents statutaires.

Ces cadres sont fixés par :

- l'arrêté royal du 12 novembre 1993 pour le personnel des services extérieurs;
- l'arrêté royal du 6 avril 1995 pour le personnel de l'Administration Centrale du ministère de la Justice.

Le Comité R recommande aussi :

- que tous les emplois administratifs de la Sûreté de l'Etat soient en principe réservés à des agents statutaires;
- que le recours à des agents contractuels dans ce service soit, autant que possible, réservé : à des emplois d'experts-analystes au sens de l'article 1^{er}, 20^o de l'arrêté royal du 1^{er} février 1993 à des emplois du niveau 4 (ouvriers et agents d'entretien);
- que la mobilité soit appliquée aux agents des services extérieurs de la Sûreté de l'Etat conformément aux nouveaux textes qui régissent cette matière dans le statut des agents de l'Etat;
- que des mesures légales règlent l'octroi des certificats de sécurité aux membres des services de renseignements ⁽³⁾;
- que l'exécution des enquêtes de sécurité soit toujours réalisée avant l'entrée en fonction des agents concernés, et ce, avec leur accord ⁽⁴⁾;

⁽³⁾ Cfr. recommandations du Comité consécutives à l'enquête sur les certificats de sécurité, rapport d'activités de 1995, p. 134 (F).

⁽⁴⁾ Idem

- que les dossiers de tous les agents de la Sûreté de l'Etat contiennent au moins une copie de l'avis donné par l'administrateur général de ce service en vue de l'agrément des candidatures par le ministre de la Justice.

10. ECHANGE DE VUE AVEC LE MINISTRE DE LA JUSTICE

Le ministre de la Justice a été mis en possession d'un projet de rapport adressé sous forme provisoire et sous pli confidentiel le 20 novembre 1996. Il lui a été demandé d'organiser un échange de vues sur la question conformément à l'article 33, alinéa 5 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement.

Par sa lettre du 12 mars 1997, le ministre de la Justice a accusé réception dudit rapport provisoire. Il déclare avoir pris bonne note de ses conclusions et avoir demandé une analyse de ses services administratifs.

“Il apparaît en premier lieu que toute les matières relatives au personnel ressortent à la compétence de la direction des ressources humaines et matérielles sous l'autorité de Monsieur le Secrétaire général. J'ai donc l'intention d'interroger celui-ci avant de vous transmettre mes observations relatives aux conclusions de votre Comité”.

Le ministre de la Justice justifie aussi l'engagement d'une personne en qualité d'expert, au sujet duquel le Comité R se posait des questions.

Le ministre déclare enfin qu'il partage le souci exprimé par le Comité pour qu'il soit effectivement pourvu au cadre organique par du personnel statutaire.

CHAPITRE 3 : LA COORDINATION DES SERVICES DE RENSEIGNEMENT

1. PROCÉDURE

En réunion du 21 janvier 1997, le Comité R a décidé d'ouvrir d'initiative une enquête concernant la coordination des services de renseignement.

Un membre du Comité a été chargé de suivre cette enquête et d'en faire rapport régulièrement au Comité.

L'ouverture de cette enquête a été notifiée à messieurs les Présidents du Sénat et de la Chambre des représentants en date du 27 janvier 1997.

Le chef du Service d'enquêtes a été chargé de mener à bien cette enquête par apostille du 26 mars 1997.

Le 2 avril 1997, le chef du Service d'enquêtes a informé les ministres compétents de l'ouverture de cette enquête.

2. FONDEMENT DE L'ENQUÊTE

Une des missions décrites dans l'article 1er de la loi du 18 juillet 1991 stipule que le Comité R a pour mission d'assurer la coordination et l'efficacité des services de renseignement.

Ce sujet d'enquête avait déjà été abordé par le Comité R dans son rapport annuel d'activités 1995⁽¹⁾. Il s'agit pour lui d'une préoccupation permanente.

Le Parlement s'intéresse aussi à ce sujet.

3. L'INTERET PARLEMENTAIRE POUR LE PROBLÈME

3.1. L'intérêt des commissions d'enquête parlementaire

L'enquête parlementaire "*sur la manière dont la lutte contre le banditisme et le terrorisme est organisée*" concluait que la collaboration entre la Sûreté de l'Etat et les instances externes était organisée de manière informelle et imprécise. La commission estimait qu'il convenait d'organiser cette collaboration sur une base impérative et que le contrôle du Gouvernement devait être

⁽¹⁾ Rapport général d'activités 1995, Titre III- p. 148 et suivantes

structuré. *“Il serait en outre opportun de prévoir qu’il y ait un échange d’informations entre la Sûreté de l’Etat et le Service général du renseignement et de la sécurité de l’armée”.* (Chambre des représentants, s.o. 1989-1990, 30 avril 1990 - 59/8 - 1988, chapitre IX F.pp. 371 et 374)

Le rapport de l’enquête parlementaire *“sur l’existence en Belgique d’un réseau de renseignements clandestin international”* (Sénat - 1^{er} octobre 1991 - 1117 - 4, session 1990- 1991, p. 29) fait état d’un Comité “inter-services” créé en 1970-1971 afin d’harmoniser des actions du SDRA VIII et du STC/Mob dans l’organisation du réseau “Stay-Behind”. Les conclusions de cette enquête sont notamment que *“le partage des tâches et des responsabilités entre les services dits militaire et civil suppose l’existence de structures de coordination à l’initiative des ministres concernés (...). Une coordination par les services eux-mêmes ne peut qu’aboutir à renforcer leur indépendance, ce qui exclut toute responsabilité politique de la part des ministres compétents.*

3.2. Les questions parlementaires

Le Comité R a recensé neuf questions parlementaires ayant trait à la collaboration et à l’échange d’informations entre le SGR et la Sûreté de l’Etat.

Au cours de l’année 1988, le député Van Dienderen (AGALEV) a posé plusieurs questions relatives à la surveillance des associations pacifistes par le SGR. A l’occasion de deux de ces questions au moins (questions n° 45 du 18 mars 1988 et n° 37 du 8 juillet 1988 au ministre de la Défense nationale), le député a demandé si des informations étaient échangées entre le SGR et la Sûreté de l’Etat sur le mouvement pacifiste.

Réponse du ministre de la Défense nationale (extrait) : *“les définitions des groupements subversifs et des groupements potentiellement subversifs sont identiques à celles émises par le ministre de la Justice, et adoptées par la Gendarmerie et la Sûreté de l’Etat. D’autre part, l’échange de données concernant les organisations subversives ou potentiellement subversives entre les différents services de sécurité , n’est pas systématique. Il est limité aux strictes nécessités que requière l’efficacité de ces services”.*

La question n° 383 posée par Mme Vogels (AGALEV) au ministre de la Justice le 21 février 1990 est relative à l’échange de données de la Sûreté de l’Etat avec d’autres services. Elle comporte notamment les volets suivants : *“Quelles informations concrètes concernant des personnes, groupements et événements ayant trait à la sécurité militaire la Sûreté de l’Etat échange-t-elle avec les services de sécurité militaire (SGR) ? Selon quelles procédures, par le biais de quels comités et de quelle manière ? Pourquoi, depuis quand et sur la base de quelles directives”.*

Réponse du ministre de la Justice (extrait) : après avoir rappelé la mission de la Sûreté de l’Etat, le ministre déclare : *“Il découle de cette mission générale qu’elle informe de ce qui peut les intéresser les services chargés du maintien de l’ordre public, de la lutte contre le terrorisme, de la sécurité de certaines institutions et de l’application des règlements sur les informations classifiées. A leur tour, ces services informent la Sûreté de l’Etat de certaines affaires qui appartiennent à son terrain d’action. La plupart du temps, cet échange de données a lieu en application de procédures et règlements administratifs”.*

Et le ministre de citer la collaboration avec le Groupe interforces anti-terroriste qui a fait l’objet d’une instruction ministérielle en 1984.

“Les renseignements qui peuvent être importants en vue de la sécurité de certaines institutions sont également fournis aux services de renseignement et de sécurité militaire”.

Les 10 avril 1992, 29 septembre 1992 et 8 janvier 1993, M. Eerdeken (PS) a posé aux ministres de la Justice et de la Défense nationale les questions n° 22, 45, 164 et 221. Celles-ci avaient trait aux activités d'extrême droite d'un sous-officier de carrière à la force terrestre et à l'échange de données auquel les services de renseignement ont procédé à propos de cet individu.

Des réponses ministérielles, il ressort que tant le SGR que la Sûreté de l'Etat étaient au courant des activités extrémistes du sous-officier et que la Sûreté de l'Etat a communiqué des informations au SGR à ce sujet.

La question n° 162 posée par M. Boutmans (AGALEV) au ministre de la Justice en date du 24 mai 1996 a trait au rapport du Comité R relatif à un trafic d'armes vers l'Iraq⁽¹⁾. La question comporte notamment le volet suivant : *"Le service de la sécurité militaire n'est-il pas tenu lorsqu'il reçoit des informations sur une affaire de trafic d'armes, d'échanger des données relatives à ce trafic avec la Sûreté de l'Etat, dont les nouvelles missions concernent précisément en première instance le trafic d'armes"*.

Réponse du ministre de la Justice (extrait) : *"S'il n'existe aucune obligation pour un service de transmettre des informations à un autre service, il convient cependant d'encourager l'échange d'informations et de mieux coordonner l'action des services de renseignements"*.

M. Boutmans a posé les mêmes questions au ministre de la Défense nationale le 28 mai 1996 (question n° 37). Il demande en plus : *"Pourquoi le SGRS s'est-il abstenu d'informer la Sûreté de l'Etat dans cette affaire de trafic d'armes, alors que cette matière fait expressément partie des nouveaux domaines d'investigation de la Sûreté de l'Etat ? N'y a-t-il pas de directives à ce sujet ? Quelles sont les règles qui régissent la collaboration et les échanges d'informations entre ces deux services ?"*.

Réponse du ministre de la Défense nationale (extrait) : *"Sur la base des idées émises dans l'avant projet de loi organique des services de renseignement, les cabinets préparent un protocole d'accord de coordination et de coopération entre les deux services"*.

4. OBJET DE L'ENQUÊTE

Le Comité R, exerçant son contrôle a posteriori, s'est intéressé à l'évolution de la coordination des services de renseignement depuis 1995 et a posé les questions suivantes aux chefs des services contrôlés :

1. A propos de quels sujets, intérêts militaires stratégiques ou liste des mouvements suivis, les services de renseignement ont-ils coordonné leurs activités de fin octobre 1995 à avril 1997 ?
2. De quelle manière ?
3. Comment cette coordination s'est-elle traduite ? Par des directives ? Sur le terrain ?
4. Le Comité R souhaite que les réponses ne se limitent pas à des généralités, il vous prie en conséquence d'étoffer les réponses avec des éléments concrets.
Combien de fois les agents se sont-ils rencontrés ? Combien de notes furent-elles échangées ? Des rapports communs ont-ils été rédigés ?

⁽¹⁾ Rapport d'activités 1995 - p. 140

5. Un accord est-il en cours d'élaboration, est-il signé et approuvé par les ministres compétents ?

Au cours de l'enquête, le Comité R a appris que les services contrôlés avaient signé un protocole d'accord. Ce document fait l'objet d'une analyse du Comité R, reprise dans la seconde partie de la synthèse de cette enquête.

Le 26 mai 1997 une réunion s'est tenue au Comité R à laquelle ont participé les chefs des services contrôlés. Cette réunion avait pour objectif de répondre aux interrogations du Comité R sur la problématique examinée, d'analyser ensemble le protocole d'accord et la mise en application des arrêtés royaux créant le Comité ministériel du renseignement et de la sécurité (arrêté royal du 21 juin 1996 - Moniteur belge du 5 septembre 1996 p. 23.492) et du collège de renseignement et de la sécurité (arrêté royal du 21 juin 1996 - Moniteur belge du 5 septembre 1996 page 23.492).

5. SYNTHÈSE DE L'ENQUÊTE

5.1. La coordination d'octobre 1995 à février 1997

Par courrier du 4 juin 1997, l'administrateur général de la Sûreté de l'Etat a donné les réponses suivantes :

"A la suite de la réunion du 26 mai 1997 au siège du Comité R, je suis en mesure de vous faire savoir, après concertation avec le général-major Simons, qu'entre octobre 1995 et février 1997, la signature du protocole a été préparée en fonction de la spécification des compétences respectives des services de renseignements, ainsi qu'elles ont finalement été établies au projet de loi sur les services de renseignements.

Il n'y a pas eu de directive transitoire et les réunions et contacts se sont poursuivis en fonction des événements.

Cependant, il n'a pas été établi un inventaire de ces contacts et je ne suis, par conséquent, pas en mesure de répondre aux questions détaillées formulées dans le questionnaire adressé le 26 mars 1997 au chef du service d'enquêtes du Comité R."

La réponse du chef du SGR en date du 13 juin 1997, un peu plus étayée que celle de l'administrateur général de la Sûreté de l'Etat, est la suivante :

"1. Jusque et y compris 1995, la collaboration entre la Sûreté de l'Etat et le SGR ne peut être qualifiée de systématique et organisée. Les contacts eurent lieu sur une base "ad-hoc" et dirigée sur des problèmes de terrain concrets.

2. Depuis fin 1995, les deux services de renseignement ont fourni un effort important en vue d'aboutir à la signature d'un protocole d'accord portant sur la coordination et la collaboration entre la Sûreté de l'Etat et le SGR. L'aboutissement de cet effort s'est concrétisé par la signature dudit protocole le 20 février 1997, protocole approuvé ultérieurement par les ministres compétents.

3. Une réflexion intense s'est poursuivie entre le SGR et la Sûreté de l'Etat aussi bien à l'occasion de rencontres entre les chefs des Services qu'au cours de l'élaboration des textes effectuée par les collaborateurs et ce en concertation préalable dans les mois qui ont précédé la signature du protocole.

4. *Afin de donner le plus possible une voix au chapitre aux différentes sections, qui devront en fin de compte mener à bien pratiquement la coordination, chaque chef de service au sein du SGR a été prié de faire des commentaires sur le projet de protocole. Ainsi, à plusieurs reprises de nouvelles propositions de textes ont été échangées avec la Sûreté de l'Etat.*
5. *L'application du protocole d'accord a fait l'objet de manière pragmatique de deux notes internes :*
 - a. *Note SGR/S/0082/97 du 22 avril 1997(annexe A)*
 - b. *Note du SGR/9713063 (annexe B)*
6. *Depuis la signature du protocole d'accord, des réunions de coordination entre les Services ont eu lieu régulièrement. Le calendrier de ces réunions a été fixé, comme prévu dans le protocole d'accord, par la Sûreté de l'Etat pour les six premiers mois de l'année 1997. L'annexe B donne une vue d'ensemble des sujets et des dates auxquelles les réunions se sont tenues.*
7. *En dehors de cette collaboration portant sur la préparation du protocole de collaboration, une réunion a eu lieu le 18 octobre 1996 entre les deux services à propos de la problématique de la sélection et de la destruction des dossiers. Au cours de cette réunion les deux services ont eu l'occasion d'exposer les principes propres à la tenue et la destruction des dossiers.*⁽¹⁾*

Le Comité R a eu l'occasion de vérifier au cours des quatre années écoulées depuis sa mise en place que la collaboration et la coordination des services de renseignement n'ont pas été assurées de façon systématique malgré le voeu du législateur.

Lors de la réunion du 26 mai 1997 les chefs des services de renseignement ont donné les explications suivantes :

- Suivant l'administrateur général de la Sûreté de l'Etat, la collaboration des deux services existait sur le terrain mais elle n'a été régie par aucune directive écrite.
- Le chef du SGR indique que des réunions ont eu lieu entre les deux services et que des documents ont été échangés, sans autre précision.

Le Comité R constate que la collaboration et la coordination des services prennent un tournant positif grâce au protocole d'accord signé le 20 février 1997 entre les responsables des services contrôlés et approuvé ultérieurement par les ministres compétents.

Le Comité R se réjouit véritablement de la collaboration et de la coordination des services. Car, souvent par le passé, il avait déploré certaines carences dans des enquêtes ponctuelles telles que notamment l'enquête sur l'exploitation d'une information fournie par un informateur au SGR, l'enquête sur l'efficacité des services de renseignement relative à l'activité des sectes en Belgique, l'efficacité et la coordination des services de renseignement à propos des événements dramatiques au Rwanda, la destruction de documents de la Sûreté de l'Etat et du SGR, et de façon plus pointue à l'occasion d'une réunion que le Comité R a organisée sur la coordination des services de renseignement en 1995.

⁽¹⁾ Traduction libre

La création du Comité ministériel du renseignement et de la sécurité et du collège du renseignement et de la sécurité constituent indiscutablement des outils indispensables à la bonne exécution par le pouvoir exécutif de la décision du pouvoir législatif d'assurer une réelle collaboration et coordination des services de renseignement.

5.2. Le protocole d'accord signé le 20 février 1997 par les chefs des services de renseignement

Le 28 avril 1997 et le 5 mai 1997, les responsables des services contrôlés ont transmis d'initiative, en application de l'article 33 de la loi organique de contrôle permanent des services de police et de renseignements, le protocole d'accord entre le SGR et la Sûreté de l'Etat portant sur la collaboration et la coordination des deux services contrôlés.

Le protocole d'accord a été élaboré à l'initiative et sous la direction des ministres compétents qui l'ont approuvé après le 20 février 1997.

"Le protocole d'accord entre le ministre de la Justice et le ministre de la Défense nationale réglant la coopération et l'échange d'informations entre la Sûreté de l'Etat et le Service Général du Renseignement et de la sécurité" étant classifié confidentiel, le Comité R estime ne pas pouvoir en révéler publiquement la teneur au risque de porter préjudice à l'efficacité des services contrôlés.

Le Comité R ayant analysé ce document peut toutefois préciser que ce protocole d'accord a pour objet :

"- d'assurer la coordination des activités ;

- de faciliter et de stimuler l'échange de documents et d'informations ;

- d'organiser la coopération ;

- d'intensifier l'échange d'idées et d'analyses ;

- de résoudre d'éventuels conflits de compétence dans les domaines de compétence mixte."

Les six chapitres de ce document et ses deux annexes concernant les dispositions pratiques ont été examinés et discutés avec les deux responsables des services contrôlés.

De manière générale le Comité R estime que les constatations suivantes peuvent être faites :

1. En ce qui concerne le crime organisé, le Comité R estime qu'il peut aussi mettre en danger les forces armées sans que des militaires y soient impliqués, par exemple à l'occasion de gros contrats de fournitures militaires, en cas de voisinages malsains à proximité d'installations militaires.

Les chefs des services de renseignement admettent le point de vue du Comité R.

2. Un membre du Comité R se demande si la prolifération des armes non conventionnelles, nucléaire, biologique et chimique, ne relève pas plutôt des compétences du SGR que de celles de la Sûreté de l'Etat.

Le chef du SGR répond que c'est une matière extrêmement importante pour la sécurité de

la défense mais ce n'est pas parce qu'il est question d'armes que le SGR est nécessairement compétent.

L'administrateur général de la Sûreté de l'Etat déclare qu'en cette matière, le fait que des intérêts économiques nationaux soient en jeu n'est pas de nature à faciliter le travail. Sur base de ces explications le Comité R estime quant à lui que cette matière devrait relever aussi de la compétence du SGR en Belgique qui devrait optimiser la recherche en ce domaine avec toutes les collaborations possibles. Le ministre de la Défense nationale devrait prévoir un renforcement des effectifs dans cette section du SGR.

3. Le Comité R plaide pour une utilisation en commun des sources ouvertes par les services de renseignement, ceci pour réduire les coûts.

Une réunion commune s'est déjà tenue entre la Sûreté de l'Etat et le SGR à propos d'Internet. L'inventaire des moyens disponibles et des moyens souhaités a été dressé. Les cadres des services de renseignement ne prévoient pas encore d'informaticien.

Dans les services de renseignement, on admet que 80 à 90 % des informations nécessaires à un service de renseignement peuvent être trouvées sur des sources ouvertes. Cependant, en situation de crise, le renseignement HUMINT est primordial car il permet entre autres de connaître la situation en temps réel, et non pas le lendemain par les journaux.

Le Comité R ne peut que répéter à cet égard les recommandations qu'il formule dans le rapport d'activités de 1996 p. 230 :

"Le Comité R propose de créer une unité de sources ouvertes communes aux deux services de renseignement. Cette proposition constitue un instrument pour une véritable collaboration des services de renseignement.

Cette proposition comporte deux volets dans un premier temps :

- 1° *Elargir le service de documentation générale par l'engagement d'analystes. Ce service devra fonctionner comme unités de source ouvertes et répondre endéans un bref délai aux demandes d'information, provenant d'analystes des différentes divisions. Le résumé des informations permet de disposer d'une vue globale du contexte dans lequel se situe le sujet traité.*
- 2° *La mise à disposition des services de moyens suffisants. Un bon équipement informatique est indispensable. Des abonnements à des bases de données commerciales et à des bibliothèques peuvent également être d'une grande utilité."*

4. Le Comité R soulève alors les nouvelles compétences prévues par le projet de loi organique sur les services de renseignement et de sécurité : le renseignement relatif aux menaces contre le potentiel scientifique ou économique du pays.

L'administrateur de la Sûreté de l'Etat estime qu'il s'agit bien d'une mission à caractère civil susceptible d'être confiée à la Sûreté de l'Etat mais qu'il lui faudrait des effectifs supplémentaires pour l'accomplir.

Le SGR devrait collaborer à cette mission lorsque la sécurité des forces armées ou des installations de la Défense nationale sont concernées. Une concertation sera nécessaire entre le SGR et la Sûreté de l'Etat sur ce sujet. Le chef du SGR estime aussi que son

service ne dispose pas actuellement de moyens suffisants pour prendre part à des missions supplémentaires.

Le Comité R estime que le pouvoir exécutif ne peut, sous peine de manquer de réalisme et de mener une politique incohérente, augmenter les compétences des services et réclamer de leur part une plus grande efficacité sans mettre des moyens supplémentaires à leur disposition.

5. Un membre du Comité R estime qu'il y a un certain déséquilibre entre les obligations de la Sûreté de l'Etat et celles du SGR. Les obligations du SGR en matière de communication d'informations à propos de trois des sujets traités par chacun des services sont plus importantes que pour la Sûreté de l'Etat. Ce fait, qui n'est pas contesté par les parties prenantes au protocole d'accord, trouve son origine dans la volonté de limiter le SGR à son terrain d'action traditionnel : la sécurité militaire.

Ce membre estime quant à lui qu'il ne s'agit pas d'une extension de compétence mais qu'il convient de s'échanger le plus grand nombre d'informations possible afin de pouvoir diffuser le renseignement en ayant pu analyser la situation de manière globale. Se limiter dans les sources d'informations peut entraîner pour le SGR une moins bonne analyse de la situation et donc porter atteinte à l'efficacité du SGR.

5.3. La mise en place du Comité ministériel du renseignement et de la sécurité et celle du Collège du renseignement et de la sécurité

Le Collège du renseignement et de la sécurité s'est déjà réuni plusieurs fois depuis juin 1996, date de sa création.

On a examiné la façon dont les différentes informations seront échangées entre les services qui y sont présents (Sûreté de l'Etat, SGR, Gendarmerie, Police générale du Royaume et ministère des Affaires étrangères).

Il s'agit d'une approche systématique pour aboutir à un rapport de synthèse approuvé par le Collège avant d'être transmis au Comité ministériel.

A l'issue de chaque réunion, l'ordre du jour de la réunion suivante est fixé à l'initiative du président : le chef de cabinet du Premier ministre. Chaque service représenté au Collège peut bien sûr proposer de mettre certains points à l'ordre du jour.

Ainsi, le problème des trafics d'armes conventionnelles et N.B.C. constitue un problème énorme avec des enjeux économiques et financiers considérables. Le ministère des Affaires économiques est aussi concerné par le problème.

Le Comité R constate que le Collège du renseignement et de la sécurité, outil indispensable à une bonne collaboration et coordination des services de renseignement, devient peu à peu opérationnel.

6. CONSTATATIONS

Le Comité R a eu l'occasion de vérifier au cours des quatre années écoulées depuis sa mise en place que la collaboration et la coordination des services de renseignement n'ont pas été assurées de façon systématique malgré le vœu du législateur.

Le Comité R constate qu'elles prennent un tournant positif grâce au protocole d'accord signé le 20 février 1997 entre les responsables des services contrôlés et approuvé ultérieurement par les ministres compétents.

Le Comité R estime que le crime organisé peut aussi mettre en danger les forces armées sans que des militaires y soient impliqués, par exemple à l'occasion de gros contrats de fournitures militaires, en cas de voisinages malsains à proximité d'installations militaires.

Le Comité R constate que la prolifération des armes nucléaires, biologiques et chimiques en Belgique relève de la compétence de la Sûreté de l'Etat et à l'étranger du SGR.

Les deux services de renseignement se voient attribuer de nouvelles compétences par le projet de loi organique sur les services de renseignement et de la sécurité sans que des moyens en personnel et en matériel ne leur soient conférés pour la bonne exécution des dites missions.

Le Comité R constate que le Collège du renseignement et de la sécurité, organe créée par arrêté royal du 21 juin 1996 constitue un outil indispensable à une bonne collaboration et coordination des services de renseignement et qu'il devient peu à peu opérationnel.

Un membre du Comité R estime qu'il y a un certain déséquilibre entre les obligations de la Sûreté de l'Etat et celles du SGR. Les obligations du SGR en matière de communication d'informations à propos de trois des sujets traités par chacun des services sont plus importantes pour le service militaire que pour le service civil de renseignement.

7. RECOMMANDATIONS

Le Comité R recommande que le protocole d'accord reconnaisse que le crime organisé est également de la compétence du SGR lorsqu'il menace la sécurité et l'intégrité des forces armées.

Sur base de ces explications fournies par les chefs des services contrôlés le Comité R estime que la prolifération des armes nucléaires, biologiques et chimiques devrait relever aussi de la compétence du SGR en Belgique qui devrait optimiser la recherche en ce domaine avec toutes les collaborations possibles. Le ministre de la Défense nationale devrait prévoir un renforcement des effectifs dans cette section du SGR.

Le Comité R comprend parfaitement les remarques des chefs des services contrôlés en ce qui concerne les nouvelles compétences attribuées à leur service. Il ne peut qu'approuver et soutenir leur légitime revendication de voir les ressources humaines de leur service s'accroître.

Le pouvoir exécutif ne peut, sous peine de manquer de réalisme et de mener une politique incohérente, augmenter les compétences des services et réclamer de leur part une plus grande efficacité sans mettre des moyens supplémentaires à leur disposition.

Un membre du Comité R recommande que le protocole d'accord soit revu afin de rétablir l'équilibre qui doit nécessairement présider entre les obligations réciproques des services de renseignement. Il apparaît manifestement que le SGR se voit contraint de fournir plus d'informations à la Sûreté de l'Etat que l'inverse.

Se limiter dans les sources d'informations peut entraîner pour le SGR une moins bonne analyse de la situation et donc porter atteinte à l'efficacité du SGR.

CHAPITRE 4 : BELINFOSEC

SUITE DE L'ENQUÊTE MENÉE DEPUIS 1994 SUR LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Dans son rapport d'activités de 1994, le Comité permanent de contrôle des services de renseignement avait déjà attiré l'attention du Parlement sur l'importance du problème : il avait recommandé qu'un organisme officiel soit chargé de concevoir et d'appliquer une politique globale de sécurité des systèmes d'information pour l'ensemble de la fonction publique.

L'enquête, ouverte le 13 juin 1994, avait initialement pour objet de déterminer qui, en Belgique, évalue le degré de sécurité du matériel et des systèmes de chiffrement ainsi que des systèmes d'information. Il s'agit de savoir s'il existe en Belgique un service officiel qui :

- produit, évalue et contrôle les systèmes de chiffrement;
- délivre des certificats de sécurité pour ce type de matériel;
- en contrôle l'usage et la commercialisation;
- sensibilise les autorités, les fonctionnaires, la police, le monde judiciaire et l'industrie sur ces questions;
- effectue des études à long terme;
- forme du personnel spécialisé en la matière;
- établit des standards, harmonise les méthodes, les programmes et le matériel.

Dans la négative, l'enquête devait déterminer si des propositions ont été formulées en la matière et en évaluer les résultats éventuels. Les deux premiers rapports sur cette enquête figurent dans les rapports d'activités du Comité R des années 1995 et 1996.

Ayant présidé les travaux du groupe Belinfosec au cours de l'année 1995, le Comité R a fait siennes les conclusions adoptées par ce groupe le 11 avril 1995 et intitulées : *"la sécurité des systèmes d'information : une préoccupation gouvernementale ?⁽¹⁾"*. Ce texte, accompagné des conclusions et recommandations du Comité R, a été transmis au Parlement ainsi qu'à

⁽¹⁾ Comité R - rapport d'activités 1995 - pp. 103 à 106

messieurs les ministres de la Justice et de la Défense nationale le 25 juillet 1995. L'élaboration et la mise en oeuvre d'une réglementation en matière de systèmes d'information relèvent en effet de la compétence du Gouvernement.

Le Comité R a souhaité que la recherche de solutions se poursuive dans la transparence et qu'elle soit accompagnée d'un large débat public. Les recherches et débats au sein du groupe Belinfosec répondant à ce souhait du Comité R, il a dès lors continué à suivre les travaux de ce groupe en qualité d'observateur. Dans cet esprit, le Comité R s'est engagé à relayer les propositions du groupe Belinfosec auprès du Parlement.⁽²⁾

Cette année, le Comité R souhaite porter à la connaissance du Parlement l'étude ci-après qui a été réalisée par le groupe juridique de Belinfosec. Cette étude est intitulée "*Les aspects juridiques de la sécurité de l'information - écoutes, prise de connaissance et enregistrement de communications et télécommunications privées et usage de la cryptographie en droit belge*". Le Comité R se rallie aux conclusions de cette étude, à savoir :

- l'urgence à vouloir réglementer l'usage du chiffrement est souvent mauvaise conseillère;
- l'internationalisation des communications exige que les questions relatives à la sécurité informatique, et plus particulièrement à la cryptographie, soient traitées sur un plan supranational;
- eu égard à l'analyse des différentes solutions existantes, le principe du contrôle "a posteriori" est celle qui présente le plus d'intérêt.

Dans cette enquête, le Comité R s'en tient à un rôle de réflexion et de recommandation qui est de sa compétence. Cette compétence couvre notamment le fait d'attirer l'attention du Parlement sur la nécessité de mener une réflexion sur la manière de doter notre pays de textes légaux et de structures adéquates. Il s'agit pour lui d'un débat important sur la société de l'information dans lequel se pose notamment la question du rôle que doivent y jouer les services de renseignements et avec quels moyens.

⁽²⁾ Comité R - rapport d'activités 1996 - p. 66

BELINFOSEC

GROUPE JURIDIQUE

LES ASPECTS JURIDIQUES DE LA SECURITE DE L'INFORMATION

ECOUTES, PRISE DE CONNAISSANCE ET ENREGISTREMENT DE
COMMUNICATIONS ET TELECOMMUNICATIONS PRIVEES ET USAGE DE LA
CRYPTOGRAPHIE EN DROIT BELGE

ETUDE DE L'EXISTANT ET PERSPECTIVES

RAPPORT FINAL

Coordination: Antoine Mireille (CRID)

Membres: Agro Juliette (Belgacom) - Antoine Mireille (CRID - CITA) - Delos Olivier (Belgacom) - Gony Michel (Belgacom) - Makedonsky Igor (IBPT) - Quisquater Jean-Jacques (UCL Unité de Micro-Electronique) - Ramaekers Jean (Institut d'Informatique - FUNDP) - Van Bulck Ivo (BVB/ABB) - Van Eecke Patrick (ICRI) - Voet Ann (IBM) - Verlackt Wouter (Fabrimetal) - Wynant Patrick (BVB/ABB).

ECOUTES, PRISE DE CONNAISSANCE ET ENREGISTREMENT DE COMMUNICATIONS ET TELECOMMUNICATIONS PRIVEES ET USAGE DE LA CRYPTOGRAPHIE EN DROIT BELGE

La sécurité de l'information peut être envisagée sous différents angles. Dans ce document, nous nous concentrerons sur l'usage des techniques cryptographiques pour assurer la confidentialité des télécommunications⁽¹⁾. Le problème le plus urgent à traiter est celui de la cryptographie en rapport avec la loi sur les écoutes des communications et télécommunications privées en raison de l'ambiguïté de la législation actuelle et de l'insécurité juridique qu'elle engendre.

Précisons préalablement qu'en égard à la haute technicité de ce sujet, les aspects tant juridiques que techniques de la cryptographie ne pouvaient être dissociés et que, de ce fait, le document élaboré par le groupe juridique reflète cette interaction entre le droit et la technique,

La première partie de ce rapport consiste en l'analyse de la législation régissant la cryptographie en la replaçant dans son contexte (Constitution et Convention européenne des Droits de l'Homme). La deuxième partie traite, en détail, sous l'angle juridique et technique, des différentes solutions envisageables. Enfin, la troisième partie énonce les différents principes dont la prise en considération devrait s'avérer indispensable pour l'élaboration de règles relatives au chiffrement.

I. ÉTAT DE LA LÉGISLATION ACTUELLE EN MATIÈRE DE CRYPTOGRAPHIE

Une manière efficace d'assurer la sécurité des informations transmises par voie numérique consiste à les chiffrer. Si cette technique de sécurisation des informations offre de multiples avantages, elle peut toutefois poser des problèmes dans le cas d'écoutes pratiquées dans le cadre de la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées.

C'est sur cette dernière qu'il convient de s'attarder afin de mieux appréhender la problématique de la cryptographie en droit belge (1). Sa lecture doit être complétée par celle des articles 202 et 203 de la loi du 21 décembre 1994 portant des dispositions sociales et diverses, venant amender la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (2), Enfin, l'analyse de la Constitution et de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales permettra d'apporter un éclairage complémentaire à la problématique (3).

⁽¹⁾ Notons dès à présent que les techniques cryptographiques sont utilisées dans d'autres situations que celles résultant de la volonté de protéger la vie privée des intervenants. Tel est le cas des services cryptés pour lesquels le cryptage du signal est effectué afin d'assurer le paiement d'une redevance. On retrouve dans cette catégorie les services de radiodiffusion cryptés par câble, par voie hertzienne ou par satellite, les services de télévision numérique, de pay-per-view, near video on demand, video on demand, livraison de jeux à la demande, services d'information multimédia,...

Dans le cas de ces services, les techniques de chiffrement sont utilisées dans le but de lutter contre la réception illicite et de protéger ainsi la valeur du service presté contre rémunération. Cette différence a entraîné au niveau national et international des solutions réglementaires qui diffèrent sensiblement notamment au niveau des actions et des sanctions.

1. Loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées.

Cette loi s'inscrit dans le prolongement de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et a pour objectif de consacrer le principe de la protection de la vie privée contre les écoutes tout en autorisant ces dernières à titre exceptionnel et ce aux fins de répondre à la nécessité de la lutte contre le terrorisme et la grande criminalité.

La faculté d'effectuer des écoutes doit être considérée comme une dérogation au principe général d'interdiction de pratiquer des écoutes. Les cas les justifiant ainsi que la procédure dans lesquelles elles doivent être réalisées sont strictement définis par la loi⁽²⁾.

Notons toutefois que l'écoute, la prise de connaissance ainsi que l'enregistrement des communications et télécommunications doit avoir lieu pendant leur transmission et que toutes les communications ou télécommunications faisant l'objet d'une mesure de surveillance doivent être enregistrées, transcrites et, le cas échéant, traduites.

Afin que la loi sur les écoutes ne soit pas vidée de son sens, il était indispensable que, parallèlement, des adaptations au niveau de la réglementation des télécommunications aient lieu. Tel est l'objet de la loi du 21 décembre 1994.

2. Loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques

2.1. Article 70 bis⁽³⁾.

Le Roi se voit confier la mission de fixer, par arrêté délibéré en Conseil des ministres, les moyens par lesquels Belgacom et les exploitants des services non réservés qu'il désigne doivent permettre, le cas échéant et éventuellement conjointement, l'application de la loi du 30 juin 1994 sur les écoutes.

Cette adaptation s'inscrit dans le prolongement de l'article 90 quater, §2 du Code d'instruction criminelle (introduit par la loi sur les écoutes), qui prévoit la possibilité, pour le juge d'instruction, de requérir le concours technique des opérateurs de réseaux pour l'exécution d'une mesure d'écoute.

Les opérateurs ont donc l'obligation de faire en sorte que, du point de vue technique, leurs infrastructures, appareils et services puissent être écoutés.

Deux problèmes doivent encore être résolus.

1. Détermination des moyens techniques

⁽²⁾ Pour une étude plus approfondie de la question, voir H.-D. BOSLY, D. VANDERMEERSCH, "La loi belge du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et télécommunications privées", Rev. dr. pen. et crim., 1995, pp. 301-343 ; T. HENRION, "Les écoutes téléphoniques", J.T., pp. 205-213.

⁽³⁾ Voir copie du texte reprise en annexe.

Aucun Arrêté Royal fixant les conditions auxquelles les terminaux doivent répondre, afin qu'ils soient susceptibles d'être écoutés, n'a été adopté à ce jour.

2. Tarification

L'obligation de faire en sorte que les communications puissent être écoutées est considérée comme étant du ressort des opérateurs de réseau. De ce fait, la charge financière leur en incombe. Il n'en va toutefois pas de même lorsque leur intervention est sollicitée dans le cadre de la loi sur les écoutes⁽⁴⁾. Le problème de la tarification doit toutefois encore être résolu.

Par ailleurs, un problème quant à l'interprétation de l'étendue des obligations de Belgacom et des exploitants des services non réservés se pose dans la mesure où elles ne sont pas clairement définies dans la loi.

2.2. Article 95. alinéa 1er⁽⁵⁾

L'article 95, alinéa 1^{er}, figurant au chapitre VIII, "Appareils terminaux" prévoit une nouvelle possibilité pour le Ministre, sur proposition de l'Institut belge des services postaux et des télécommunications, de retirer un agrément ou imposer une interdiction de maintenir le raccordement à l'infrastructure publique de télécommunications lorsqu'il s'avère que l'appareil terminal rend inefficaces les moyens permettant l'application de la loi du 30 juin 1994 sur les écoutes.

L'application de cette disposition pose quatre problèmes.

1. Champ d'application restrictif

L'hypothèse visée est celle des terminaux pouvant assurer le chiffrement des informations. L'article 68, 7° de la loi du 21 mars 1991 susmentionnée, définissant la notion de terminal a été modifié par l'Arrêté Royal du 22 décembre 1994⁽⁶⁾ afin de faire coïncider la définition d'appareil terminal avec celle donnée par la directive 91/263/CEE.

Est considéré comme appareil terminal tout "équipement destiné à être connecté à l'infrastructure publique de télécommunications, c'est à dire :

- a) être directement connecté à un point de raccordement ou
- b) à interfonctionner avec l'infrastructure publique de télécommunications en étant connecté directement ou indirectement à un point de raccordement, en vue de la transmission ou du traitement ou de la réception d'informations, que le système de connexion consiste en fils métalliques, liaisons radio-électriques, systèmes optiques ou tout autre système électromagnétique".

Si l'on s'en tient à la définition ainsi donnée d'"appareil terminal", il apparaît que les logiciels ainsi que les appareils non terminaux pouvant assurer le chiffrement ne sont pas visés par l'article 95.

⁽⁴⁾ Exposé des motifs, Doc. Parl. Sénat, 1994-1995, 1218, 88.

⁽⁵⁾ Voir copie du texte reprise en annexe.

⁽⁶⁾ Arrêté Royal modifiant le Titre III de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, M.B. 10.02.1995, 3032

2. Absence de spécifications techniques

Dans l'état actuel de la législation, les appareils terminaux doivent permettre le repérage, les écoutes, la prise de connaissance et l'enregistrement des télécommunications privées de façon telle que leur transcription et traduction éventuelle puissent être réalisées.

Il convient de rappeler que l'agrément d'un appareil terminal doit se faire sur base de spécifications techniques fixées par arrêté ministériel (article 94, §2). Il aurait donc été suffisant de préciser au niveau de celui-ci les normes techniques nécessaires afin de rendre efficace la loi sur les écoutes téléphoniques. Le retrait d'agrément pouvait donc dans ce cas avoir lieu sur base du 2° (l'appareil ne répond plus aux spécifications techniques en vigueur). En introduisant un 5° à l'article 95, le législateur a introduit une disposition arbitraire puisque aucune norme technique justifiant un retrait d'agrément n'a été fixée.

Bien que le but visé par l'article 95 soit de garantir l'application effective de la loi sur les écoutes et non d'interdire ou de restreindre la commercialisation et l'utilisation de moyens destinés à assurer la confidentialité des communications⁽⁷⁾, on peut craindre que l'application de la législation actuelle conduise à de telles conséquences.

3. Étendue de l'obligation

Le retrait d'agrément de l'appareil terminal peut avoir lieu si ce dernier rend inefficaces les moyens permettant l'application de la loi sur les écoutes téléphoniques. La question de l'interprétation du terme "inefficace" se pose. Si l'on se réfère à l'article 90, septies du Code d'instruction criminelle, il apparaît que les enregistrements de communications ou télécommunications effectués en application de la loi doivent être intégralement transcrits et, le cas échéant, traduits.

Le fait que les communications ne soient pas directement "compréhensibles" a été envisagé par le législateur puisqu'il est donc admis qu'elles puissent nécessiter une traduction. Il n'y a donc pas de raison d'appliquer aux communications chiffrées un régime différent de celui qui est applicable aux communications tenues dans une langue étrangère dans la mesure où une traduction suffit pour rendre les communications chiffrées compréhensibles. Tout au plus pourrait-il être prévu par la loi que les clés soient fournies dans le cadre d'une procédure d'écoute.

4. Absence de précision

L'expression "rend inefficace" est très vague et très large. Elle pourrait par conséquent, non seulement inclure le chiffrement, mais également un éventail d'autres protocoles de télécommunication (compression, EDIFACT...).

3. La Constitution et la Convention européenne des Droits de l'Homme

3.1. La Constitution

⁽⁷⁾ Rapport de la commission de l'infrastructure au Sénat, Doc. Parl., Sénat, 1994-1995, 1218-9, 3.

La problématique des écoutes s'inscrit dans le cadre du secret des lettres. Les auteurs de la Constitution ont voulu protéger ce secret par l'article 22. Le secret des lettres ne peut être violé que dans des conditions strictes.

3.2. Article 8 de la C.E.D.H.

Dans le cadre de la Convention européenne des Droits de l'Homme, la question des écoutes téléphoniques peut être assimilée, par analogie, à la limitation de la liberté de correspondance. La Cour européenne a confirmé cette analogie⁽⁸⁾.

La légalité des écoutes téléphoniques doit donc être analysée à la lumière de l'article 8, §2 de la Convention⁽⁹⁾.

Le système de restriction des libertés précitées prévu par la C.E.D.H. est un système de limitation matériel. Pour qu'une restriction soit conforme aux dispositions de la Convention, elle doit satisfaire à trois conditions :

- être prévue par la loi
- constituer une mesure nécessaire dans une société démocratique
- être conçue dans l'intérêt d'un "objet de droit" protégé.

Les première et troisième conditions ne posent pas de problème. La loi doit en effet être comprise au sens large. La restriction peut donc aussi être instaurée par A.R. En ce qui concerne la problématique de l'"objet de droit", l'ingérence de l'autorité publique peut se justifier si elle est nécessaire à la sécurité nationale, à la sécurité publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

Il convient par contre de se pencher sur la deuxième condition : la menace de l'"objet de droit" comme condition au caractère "nécessaire" de la limitation. Une limitation est "nécessaire" s'il existe un "besoin social impérieux" dans l'hypothèse où l'"objet de droit" protégé serait "menacé" par l'exercice illimité du droit.

Aux termes de l'article 8, §2, l'ingérence est autorisée pour autant qu'elle soit nécessaire et qu'il y ait une menace contre la sécurité nationale, la prévention des infractions pénales,... Cette menace peut être directe ou indirecte. Quand un "objet de droit" est-il directement ou indirectement menacé ?

La Cour a estimé qu'une limitation est autorisée s'il existe un danger clair et réel ("clear and present danger") que l'"objet de droit" soit menacé.

Au fil des années, cette condition est devenue, sous l'impulsion de la Cour, un véritable critère de limitation. La condition "nécessaire dans une société démocratique" est un critère d'interprétation. Il

⁽⁸⁾ Arrêt Klaas, 6 sept. 1978, Publ. Cour, Série A, vol. 28.

⁽⁹⁾ Cette limitation de la liberté entre donc dans le champ d'application tant de l'article 8 que de l'article 10 de la C.E.D.H. (Droit à la liberté d'expression). L'article 8 doit toutefois être considéré comme la "lex specialis". Les plaintes relatives aux écoutes téléphoniques sont donc examinées à la lumière de l'article 8 §2 et non de l'article 10 §2.

est extrêmement important dans le cadre de l'analyse des Constitutions et des objectifs de limitation. La Cour a confirmé à plusieurs reprises que toute formalité, condition, limitation ou sanction devait être proportionnelle à l'objectif poursuivi.

Quoi qu'il en soit, il est clair que les écoutes téléphoniques se justifient en tant que moyen de lutte contre la criminalité à condition qu'il existe une législation adéquate dont les dispositions soient accessibles et prévisibles pour le citoyen.

En France, l'usage des écoutes téléphoniques était traditionnellement basé sur les règles générales du droit pénal et les pouvoirs dont le juge d'instruction pouvait se prévaloir dans ce cadre. Cette solution a toutefois été rejetée par les juges européens dans les Arrêts Slin et Huvig du 24 avril 1990⁽¹⁰⁾ les bases légales de ces jugements ne répondant pas à des critères de qualité suffisants.

Pour ce qui est de la réponse à la question de savoir si les mesures d'exécution prévues sont conformes à l'article 8 de la C.E.D.H., il faut se référer au chapitre II, point 1.2.2.

II. PROPOSITION DE SOLUTIONS

1. Contrôle "a priori"

1.1. Description

Dans la suite de ce texte, nous appellerons "rendre une écoute possible a priori" le fait de fournir, avant ou pendant l'émission de toute communication et dans le respect des conditions fixées par la loi, les moyens techniques permettant à l'écouteur de lever la confidentialité des messages.

La technique du "Key Escrow" s'inscrit dans cette optique. Elle impose à l'utilisateur désireux de communiquer de manière confidentielle avec un interlocuteur, de confier à une ou plusieurs entités de confiance l'information secrète autorisant la levée de la confidentialité de ses communications. Cette information secrète peut être divisée en plusieurs fragments partagés entre plusieurs entités de confiance de manière à ce que l'ensemble de ces fragments, ou un sous-ensemble de ceux-ci, soit nécessaire pour lever la confidentialité d'un message.

Il existe dans la littérature jusqu'à 35 systèmes différents de key escrow⁽¹¹⁾. La plupart de ces systèmes cherchent à trouver un compromis entre le droit à la vie privée et le principe des écoutes autorisées par la loi.

A titre d'exemple, une version simplifiée est la suivante (la version du Clipper Chip américain possède un étage supplémentaire) : l'autorité du key escrow fournit à l'utilisateur A la clé ka et enregistre la paire (user A, ka) dans sa base de données virtuelle. Lorsque A envoie un message, il émet avec le message chiffré, le chiffrement de la clé de session utilisée avec la clé ka reçue de l'autorité. Lorsque l'autorité désire déchiffrer un message envoyé par A, elle déchiffre la clé de session au moyen de la clé ka pour ensuite déchiffrer le message.

⁽¹⁰⁾ 24 avril 1990, Publ. Cour, Série A, vol. 176 A-B.

⁽¹¹⁾ D. DENNING, "Description of Key Escrow System", <http://www.cosc.georgetown.edu/~denning/crypto/Appendix.html>. This document is a companion document to "A taxonomy for Key Escrow Encryption System", Communication of the ACM, Vol. 39, n°3, March 1996.

1.2. Évaluation

La possibilité d'écoute a priori pose un grand nombre de problèmes.

1.2.1. Evaluation juridique

Comme il a été dit dans la première partie (point 2), la mesure d'écoute ne peut se justifier que si la limitation prévue par l'article 8 est "nécessaire". La question se pose de savoir si le législateur et/ou le Roi pourrait imposer la remise a priori des clés.

Indépendamment du fait que la loi n'a pas confié ce pouvoir au Roi et qu'il ne peut donc pas être adopté d'arrêté d'exécution en ce sens⁽¹²⁾, il est utile de se demander si une remise a priori des clés peut être considérée comme "nécessaire" au sens de la jurisprudence de la Cour.

Le système de protection évoqué au deuxième paragraphe de l'article 8 n'exclut pas explicitement en tant que telle l'adoption préventive de mesures restrictives visant à protéger "l'objet de droit". étant donné qu'une mesure préventive ne peut pas être "plus que nécessaire", seules des mesures préventives particulières se justifient dans certaines conditions.

Contrairement à ce qui est le cas en France par exemple, la loi belge sur les écoutes téléphoniques n'autorise pas les pratiques d'écoute préventives. Les écoutes en Belgique doivent en effet toujours être opérées par un juge d'instruction.

Compte tenu de ce qui précède, il est difficile de soutenir qu'il est "nécessaire" que les autorités disposent a priori des clés de chiffrement. Un système qui autorise le juge d'instruction à demander les moyens techniques permettant de lever la confidentialité, selon une procédure rapide et souple, chaque fois que cela se révèle nécessaire serait totalement conforme à l'objectif de la loi : rendre les écoutes possibles. Une remise a priori n'est donc pas nécessaire et est probablement contraire à l'article 8 de la C.E.D.H.

Le déposant des clés doit faire une entière confiance aux procédures de sécurité mises en place par l'autorité dépositaire, ainsi qu'à l'intégrité des personnes impliquées. Il doit aussi compter sur une politique stable de la part de cette autorité et sur une constance des lois en vigueur.

1.2.2. Evaluation technique

En contradiction avec les principes de base de la sécurité de l'information

Délimitation du message à déchiffrer

Le problème vient du fait que le juge d'instruction, en possédant la totalité des moyens techniques nécessaires pour lever la confidentialité pourrait, dans le cadre d'une procédure d'écoute, accéder à beaucoup plus d'informations que celles contenues dans le message chiffré intercepté. En effet, le

⁽¹²⁾ Il ne ressort ni du texte de la loi, ni des travaux préparatoires que le Roi serait habilité à imposer une remise a priori des clés (Sénat, 1218-1-9, 1994-1995).

fait de posséder la clé permet d'accéder aux messages antérieurs, (voire postérieurs si la clé n'est pas modifiée).

Les principes élémentaires de sécurité exigeant une distribution et une duplication minimale des secrets, ainsi qu'un stockage des secrets uniquement là où ils sont utilisés.

Le dépôt des clés doit être géré comme s'il s'agissait de déchets nucléaires : stockage hautement sécurisé, backups, destruction effective. Chacune des bases de données contenant les clés secrètes déposées représenterait une cible de choix sous la responsabilité d'une tierce personne. Le secret-sharing ou le fonction-sharing ou les solutions dites "threshold" peuvent être appliquées pour le stockage des données sensibles dans les bases de données : la base de données virtuelle est divisé en plusieurs morceaux de telle manière que 2 morceaux sur 3 (par exemple) sont nécessaires pour reconstituer la base de données (Clipper : 2 sur 2).

Il existe des circuits qui ne permettent pas d'effectuer des copies de la clé pour des raisons évidentes de sécurité. Celle-ci est scellée au sein de la carte à puce.

Il existe, de plus, des techniques spécifiques de chiffrement qui ne permettent pas une écoute partielle à la demande et nécessite l'enregistrement de la communication dans son intégralité. Même un utilisateur de bonne volonté peut ne pas être en mesure d'assurer le déchiffrement d'une partie d'un de ses messages.

L'utilisateur ne tire aucun avantage d'une solution "a priori" qu'il ne pourrait fournir lui-même. Le concept de Key Recovery constitue un problème différent.

Un exemple est celui du dépôt de clé intra-entreprise, qui suscite un intérêt évident pour les sociétés, comme solution de back-up de clés maîtres apportant ainsi une protection contre la perte ou la destruction de clés, ou contre l'indélicatesse de certains employés. Ces dépôts ont lieu, en général hors entreprise, auprès de "notaires" ou autres tierces parties de confiance. Il s'agit cependant de problèmes tout à fait différents, avec des contraintes et des objectifs différents, même si les techniques peuvent être identiques.

De nombreux problèmes techniques rendent la mise en oeuvre de telles écoutes extrêmement difficile voire impossible :

La philosophie du key escrow correspond au cas de distribution de clé secrète, du moins pour la clé maître. Cependant, la plupart des utilisateurs font usage des autres solutions impliquant des clés publiques ou dynamiques qui peuvent changer continuellement. Dans ces cas-là, un système de key escrow n'est pas efficace.

Dans un contexte international, en principe, tout pays est limité, territorialement, au niveau du droit d'écoute.

Le chiffrement additionnel de la clé de session peut être enlevé ou faussé. Il a été prouvé que le Clipper peut être faussé d'une manière telle qu'il est possible de prouver qu'un message a été envoyé par une certaine entité alors que tel n'était pas le cas. De tels problèmes se rapportant à la non répudiation doivent être résolus.

La réalisation en temps réel implique des procédures automatisées et des serveurs interconnectés utilisant un réseau hautement sécurisé.

Super-chiffrement et stéganographie :

Rien n'empêche le super ou double chiffrement : le message est lui-même le message chiffré d'un autre message original, le message réel. Ce type de manoeuvre ne peut être détecté qu'a posteriori, alors même que la preuve d'une manipulation ne pourra plus être établie. Aucune preuve de tricherie ne pourra jamais être établie.

De plus, des messages subliminaux peuvent être envoyés en utilisant la stéganographie. Celle-ci peut être définie comme étant l'art de dissimuler des secrets dans un message clair. Deux messages M (le faux message) et M' (le vrai message) peuvent être fusionnés en un seul message de telle manière que pour tous ceux qui ignorent le procédé, le message effectif sera le message bidon M. Des exemples très simples sont le montant d'un chèque qui est aussi un code pour une action à réaliser ou, encore un usage inhabituel des espaces entre les mots d'un texte, ou l'utilisation des parties invisibles des images. Ces techniques de communications ne seront jamais détectables.

2. Limitation du niveau de chiffrement

2.1. Description

Il est souvent proposé de définir des services de confidentialité prenant en compte une échelle de sécurisation par rapport à la nature de l'information à protéger :

- sécurité minimale : niveau de la lettre et de la téléphonie actuelles.
- sécurité améliorée : pour usage privé ou professionnel (niveau envois recommandés ou livraison par courrier).
- sécurité forte : information commercialement, médicalement (ou autre) sensible.

Les différents niveaux de sécurité peuvent être facilement obtenus dans la plupart des systèmes de chiffrement en jouant sur les différents paramètres de sécurité : taille de la clé, qualité de l'algorithme,...

2.2. Évaluation

2.2.1. Evaluation juridique

L'obligation légale d'employer des mécanismes de confidentialité suffisamment faibles que pour permettre les écoutes autorisées par la loi entre en contradiction totale avec les principes les plus élémentaires de la sécurisation de l'information et avec les obligations tout aussi légales qui sont faites aux gestionnaires d'informations privées, médicales, ou commercialement sensibles.

2.2.2. Evaluation générale

Aspects positifs

- pas de dépôt de clés. Dans le cas de chiffrement faible (par exemple, DES avec clés de 40 bits), il n'est pas jugé utile de procéder à des dépôts de clés vu la facilité avec laquelle ce type de chiffrement peut être cassé.

- solution peu onéreuse.
- cette solution peut être combinée avec d'autres solutions : dépôt volontaire des clés, contrôle a posteriori,...

Aspects négatifs

- solution qui ne suscite pas la confiance et qui est insatisfaisante dans les cas où une sécurité forte raisonnable doit être assurée.
- solution trop rigide. Elle ne permet pas d'adapter le niveau de sécurité en fonction des données à protéger et des risques potentiels (l'imposer comme telle serait contraire à l'article 16§3, al. 2 de la loi sur la protection de la vie privée).

3. Contrôle "a posteriori"

3.1. Description

Nous appellerons "rendre une écoute possible a posteriori" le fait de fournir, dans le respect des conditions fixées par la loi, les moyens techniques permettant à l'écouteur de lever la confidentialité des messages écoutés.

3.2. Évaluation

3.2.1. Evaluation juridique

Sur le plan juridique, cela signifie donc que, lorsque les nécessités de l'instruction l'exigent, le juge d'instruction pourrait enregistrer les communications ou télécommunications privées pendant leur transmission (comme c'est le cas à l'heure actuelle) et exiger à n'importe quel moment pendant la période de surveillance que les moyens techniques permettant l'accès au message clair lui soient communiqués. Le défaut de communication serait sévèrement sanctionné par la loi. Afin d'assurer une bonne exécution de cette mesure, les personnes utilisant des procédés techniques permettant de rendre les messages illisibles seraient tenues de conserver ces procédés pendant une durée de un mois (période pendant laquelle la surveillance peut être pratiquée) afin que la traduction des messages transmis puisse être assurée.

Notons toutefois que dans le cadre d'une instruction, les parties seraient tenues de collaborer mais qu'une telle obligation ne pourrait être transformée en obligation de résultat.

3.2.2. Evaluation générale

Aspects positifs

- la sécurité reste entre les mains de l'utilisateur. Celui-ci doit faire en sorte que les moyens techniques nécessaires pour lever la confidentialité de ses messages soient disponibles pendant une durée suffisante afin de permettre le contrôle a posteriori. L'utilisateur peut soit gérer ce problème lui-même, soit le confier à un tiers, aussi appelé tierce partie de confiance, qui le gèrera à sa place. Une telle solution s'apparente au "Key Recovery" dont question ci-dessus (Partie II, 1.2.2.) dans la mesure où le tiers de confiance n'a pas de contact direct avec l'autorité écoutante. Une telle solution ouvre la voie à d'autres perspectives : délivrance à

l'autorité écoutante, dans les conditions fixées par la loi, du message clair correspondant au message chiffré sans que celle-ci ait accès à la clé,...

- l'utilisateur a la garantie que seuls les messages enregistrés seront déchiffrés pour autant qu'il ait pris des mesures adéquates
- facilité d'application
- solution peu onéreuse
- cette solution peut être combinée avec d'autres solutions : dépôt volontaire des clefs, chiffrement faible ne nécessitant pas la communication des clefs,...

Aspects négatifs

- solution insatisfaisante dans tous les cas d'urgence
- difficulté, voir impossibilité, d'application pour certaines méthodes de chiffrement : clefs scellées (cartes à puces) génération automatique de clefs dynamiques, techniques ne permettant pas les écoutes partielles,...
- double chiffrement ou stéganographie possibles (voir supra)

III. PERSPECTIVES

Une réglementation efficace, respectant les valeurs démocratiques, ne peut être conçue en matière de chiffrement, sans la prise en considération des éléments suivants.

1. La Convention de sauvegarde des droits de l'homme et des libertés fondamentales fixe, en son article 8, § 1, le principe selon lequel "toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance", principe auquel il ne peut être dérogé dans les conditions prévues au §2 ("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, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui").

Ces principes ont notamment été réaffirmés par le Conseil de l'Europe dans la Recommandation R(95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques. Elle suggère en outre que les exploitants de réseau et les fournisseurs de services et d'équipements matériel et logiciel tirent parti "de la technologie de l'information pour fabriquer et exploiter des réseaux, des équipements et des logiciels respectant la vie privée des utilisateurs" et propose que des dispositifs anonymes d'accès au réseau et aux services de télécommunications soient mis à disposition.

2. Des travaux sont actuellement menés au niveau d'organisations internationales, que ce soit au sein de l'O.C.D.E. ou de la C.E. en témoignent notamment les différentes recommandations adoptées au niveau européen ainsi que le projet de livre vert et le livret vert respectivement

relatifs à la sécurité des systèmes d'information et à la protection des services cryptés dans le Marché Intérieur. Leur prise en considération s'impose !

3. Par ailleurs, en raison de l'internationalisation des télécommunications (et des flux transfrontières de données ainsi engendrés), les mesures qui imposent en la matière devront faire l'objet d'une harmonisation au niveau européen afin d'éviter l'émergence de "paradis de la criminalité informatique"⁽¹³⁾.
4. L'harmonisation des règles relatives au chiffrement est cruciale. On ne peut en effet à l'heure de la convergence, courir le risque d'adopter des règles contradictoires pour les émissions de radiodiffusion et les télécommunications. A cet égard, la Communication Com (96)7 6 nous paraît insatisfaisante en ce qu'elle s'applique uniquement aux émissions de radiodiffusion.
5. Quant aux solutions qui peuvent être trouvées afin de permettre l'accès aux communications téléphoniques tel qu'il est prévu par la loi du 30 juin 1994 submentionnée, elles sont multiples... et jamais totalement satisfaisantes prises individuellement. Trois critères déterminants devront guider le choix d'une solution.

- **sécurité** : aucune mesure permettant d'assurer des écoutes ne peut aboutir à la fragilisation de la sécurité. La maîtrise de la sécurité doit, en conséquence, demeurer entre

les mains de celui qui l'a adoptée. En aucun cas, directement ou indirectement, les autorités ne peuvent fragiliser ou interférer avec la sécurité relative à l'intégrité, l'authenticité et la non répudiation.

- **coût** : la solution adoptée ne peut constituer une charge financière démesurée pour toute personne physique ou morale ayant recours au chiffrement pour la sécurisation des données.
- **souplesse** : Il en va de la sécurité des télécommunications comme de celle devant garantir les données à caractère personnel : il n'existe pas une méthode absolue de sécurisation des informations. Les mesures prises en vue de garantir la sécurité des données doivent assurer un niveau de protection adéquat en fonction de la nature des communications que l'on désire protéger (voir supra II, 2.1). Par conséquent, aucune solution ne peut induire l'adoption d'un seul niveau de sécurité pour toutes les communications.

Eu égard à ces différents critères, il apparaît que la technique du "key escrow" dans le contexte d'une écoute rendue possible "a priori" est difficilement défendable tant du point de vue juridique que technique parce que, d'une part, elle constitue une mesure excessive eu égard au type d'écoute autorisée en Belgique (pour rappel, les écoutes préventives ne sont pas admises) et que, d'autre part, elle viole les principes élémentaires de la sécurité de l'information. Le coût de mise en oeuvre d'une telle solution est par ailleurs excessif eu égard au but poursuivi.

La technique du contrôle "a posteriori", en poursuivant les mêmes objectifs que le "key escrow" (déchiffrement du message) offre de plus grandes garanties, la sécurité demeurant notamment aux mains de l'utilisateur. Toutefois cette technique présente des imperfections auxquelles il conviendra d'apporter les aménagements nécessaires.

⁽¹³⁾ Y. POULET, V. WILLEMS, C. LOBET-MARIS, Vers une société de l'information, Cahier du C.R.I.D., n°10, Bruxelles, Story Scientia, 1995, p. 53.

CONCLUSION

Grâce à la loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et télécommunications privées, la vie privée des citoyens s'est vu reconnaître une protection légale efficace. Toutefois, elle autorise à titre exceptionnel, dans les cas limitativement énumérés, les écoutes lorsque celles-ci répondent à la nécessité de pouvoir lutter efficacement contre le terrorisme et la grande criminalité.

Néanmoins, le recours à certaines techniques, telles que le chiffrement, peut rendre les écoutes inefficaces, voire impossibles. Dès lors, est apparue l'idée en Belgique, comme dans beaucoup d'autres pays, de réglementer l'usage du chiffrement. L'urgence est bien souvent mauvaise conseillère. L'évaluation de la législation belge à ce sujet l'a amplement montré. Toutefois, le monde politique en a pris conscience, s'il faut en croire les deux propositions de loi récemment déposées devant le Sénat⁽¹⁴⁾.

Quoi qu'il en soit, l'internationalisation des communications exigeait que les questions relatives à la sécurité informatique, et plus particulièrement à la cryptographie soient traitées sur un plan supranational. Les règles de conduite en cours d'élaboration au sein de l'O.C.D.E., ainsi que les diverses initiatives prises au niveau de la C.E. constituent à l'heure actuelle des outils indispensables à l'élaboration d'une législation en la matière.

Enfin, au terme de cette étude, il faut souligner l'importance que revêt une initiative en matière de cryptographie. Eu égard à l'analyse des différentes solutions existantes, il apparaît que le principe du contrôle "a posteriori" est celle qui présente le plus d'intérêt.

Toutefois, tout en répondant adéquatement aux nécessités exprimées ainsi qu'aux critères précédemment énoncés (sécurité, coût, souplesse), cette technique présente des imperfections auxquelles il conviendra d'apporter les aménagements nécessaires. Tout l'art consistera à trouver cet équilibre, si précaire entre le respect du droit à la vie privée et la nécessité de la lutte contre la criminalité grave. Il y va de la fiabilité et de la crédibilité de l'évolution technologique⁽¹⁵⁾.

⁽¹⁴⁾ Proposition de loi abrogeant les articles 70 bis et 95, alinéa 1°, 5°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, Doc. Parl., Sénat, 1995-1996, 1-343/1, ; Proposition de loi abrogeant les articles 70 bis et 95 de la loi du 21 décembre 1991 portant réforme de certaines entreprises économiques et complétant le Code d'instruction criminelle afin de donner un cadre à l'aide au décryptage des messages, Doc. Parl., Sénat, 1995-1996, 1-352/1

⁽¹⁵⁾ H. MAISL, "Communications mobiles, secret des correspondances et protection des données personnelles", D.I.T., n°2, p.19.

TITRE II : NOS SERVICES DE RENSEIGNEMENT

DEUXIEME PARTIE : LES ENQUÊTES

C. SUR PLAINTE DE PARTICULIERS OU SUR DENONCIATION

CHAPITRE 1 : ENQUÊTE DE CONTRÔLE SUITE À LA PLAINTÉ DÉPOSÉE PAR MONSIEUR X

1. PROCÉDURE

Le 10 avril 1996, le Comité R a pris connaissance de la plainte qui lui a été adressée le 3 avril 1996 par monsieur X. Ce dernier se plaint qu'il a "des problèmes avec des militants néo-nazis, qu'il estime proche des services de renseignements, en particulier du SGR, en raison des fonctions politiques qu'il exerce et des activités qui en découlent."

Le 25 avril 1996, le Comité R décide, en réunion, d'ouvrir une enquête de contrôle qui portera sur les activités et méthodes du SGR suite à cette plainte.

A cette date le Comité R charge deux de ses membres de mener cette enquête et de faire rapport régulièrement au Comité R des développements de celle-ci.

Par lettre du 26 avril 1996, les présidents du Sénat et de la Chambre ont été avertis de l'ouverture de cette enquête en application de l'article 46 alinéa 3 du règlement d'ordre intérieur.

A la même date la présidente adresse aux procureurs généraux de Bruxelles et de Mons une lettre leur demandant de bien vouloir lui faire connaître la suite qu'ils ont réservée à la plainte introduite par monsieur X auprès de leurs services respectifs et ce en application de l'article 69 du règlement d'ordre intérieur.

Le 7 mai 1996 le chef du Service d'enquêtes avertit le ministre de la Défense Nationale de l'ouverture de l'enquête en application de l'article 43 alinéa 1er de la loi organique du 18 juillet 1991.

Le 15 juillet 1996 le procureur général faisant fonction à Mons écrit au Comité R en lui indiquant qu'il classe cette affaire sans suite.

Le 29 juillet 1996, le service d'enquêtes a reçu mission de convoquer le plaignant et de procéder à l'enquête.

Le 13 septembre 1996, le procureur général faisant fonction à Bruxelles écrit au Comité R en lui indiquant que la plainte de monsieur X a été jointe au dossier relatif à l'instruction judiciaire ouverte à charge de membres d'un groupe d'extrême droite. Ce dernier dossier fait l'objet de réquisitions de renvoi devant le tribunal correctionnel de Bruxelles.

Le 14 octobre 1996, le chef du Service d'enquêtes a convoqué le plaignant afin d'obtenir certaines précisions sur les reproches que ce dernier formulait à l'égard des services de renseignement et

plus précisément, de détailler de quelle façon ces services auraient de façon disproportionnée ou injustifiée, porté atteinte aux droits que la Constitution et la loi confèrent au plaignant.

Le 7 novembre 1996, le chef du Service d'enquêtes adresse un rappel au plaignant, ce dernier n'ayant pas donné signe de vie.

Le 17 janvier 1997 le Procureur général près la Cour d'Appel de Bruxelles porte à la connaissance du Comité R que la plainte de monsieur X contre monsieur Y a fait l'objet d'une procédure d'information séparée du dossier mettant en cause des membres d'un groupe d'extrême droite.

2. DÉROULEMENT DE L'ENQUÊTE

Le 28 novembre 1996 le Service d'enquêtes entend le plaignant. Monsieur X apporte divers documents à l'appui de sa plainte.

De cet entretien, il ressort que les reproches formulés par le plaignant concernent d'éventuels comportements policiers à son égard. Il précise surtout que son intention première était de laisser des traces de ses affirmations auprès d'instances officielles.

A aucun moment monsieur X n'a rapporté au Service d'enquêtes de manière concrète de quelle façon le SGR aurait porté atteinte aux droits que la Constitution et la loi lui confèrent.

Il n'a pas demandé de prendre connaissance d'un éventuel dossier le concernant auprès des services de renseignement.

Les documents remis par le plaignant ont été examinés et ont fait l'objet d'investigations. Les personnes citées par monsieur X ne font pas partie du SGR.

Le Service d'enquêtes a également pris connaissance des différents articles, parus dans la presse, au sujet des faits évoqués par le plaignant.

De l'analyse des trois éléments développés ci-dessus, il ressort que la démarche de l'intéressé s'apparente plus à une dénonciation à caractère générale sans élément probant à l'appui, qu'à une plainte spécifique.

3. CONCLUSIONS

Sur base des constatations recueillies par le service d'enquêtes, le Comité R estime que le SGR n'a en aucune façon porté atteinte aux droits que la Constitution et la loi confèrent au plaignant.

CHAPITRE 2 : ENQUÊTE DE CONTRÔLE SUITE À LA PLAINTÉ DÉPOSÉE PAR MONSIEUR Y

1. PROCÉDURE

En date du 23 octobre 1996, Monsieur Y, a adressé une lettre au Comité R, se plaignant d'un dossier qui existerait le concernant au SGR et qui lui aurait causé un préjudice moral dans ses contacts sociaux.

Lors de sa réunion du 7 novembre 1996, le Comité R a décidé d'ouvrir une enquête de contrôle portant sur l'atteinte qui aurait été portée aux droits et libertés individuelles conférés à l'intéressé.

Le Comité R a donné mission à deux de ses membres de suivre et de contrôler cette enquête et de faire rapport régulièrement au Comité R des développements de celle-ci.

Par lettre du 5 décembre 1996, les présidents du Sénat et de la Chambre ont été avertis de l'ouverture de l'enquête en application de l'article 46, alinéa 3 du règlement d'ordre intérieur.

Un accusé de réception a été envoyé à Monsieur Y le 12 décembre 1996 lui indiquant qu'il serait procédé, par le Service d'enquêtes, à son audition au sujet des reproches formulés par l'intéressé à l'égard du service de renseignement militaire.

Le 5 décembre 1996, une apostille a été adressée au chef du Service d'enquêtes le priant de:

- procéder à l'audition circonstanciée du plaignant;
- prendre connaissance et copie d'un éventuel dossier qui serait ouvert au nom de l'intéressé au SGR.

Le 5 décembre 1996 le ministre de la Défense nationale a été informé de l'ouverture de l'enquête par le chef du Service d'enquêtes conformément à l'article 43, 1^{er} alinéa de la loi du 18 juillet 1991, organique du contrôle des services de police et de renseignements.

2. SYNTHÈSE DE L'ENQUÊTE

2.1. Audition de Monsieur Y

Le Service d'enquêtes a procédé à l'audition du plaignant qui a signalé avoir été privé, entre 1979 et 1982 d'un certificat de sécurité.

Il estime qu'avoir été privé d'un certificat de sécurité, en sa qualité d'officier de réserve, à un certain moment de sa carrière, lui a causé un préjudice moral qui consiste dans le fait d'avoir été changé d'affectation lors de ses rappels sous les drapeaux, ce qui aurait affecté certains de ses rapports sociaux.

Selon l'intéressé, la mesure prise n'était basée que sur des ragots et, finalement, suite à ses nombreuses démarches, il a, selon ses dires, été "réhabilité" en 1982 et a, à nouveau, été titulaire d'un certificat de sécurité.

A l'issue de l'audition, il a été précisé à Monsieur Y que la rectification éventuelle de données à caractère personnel figurant dans le dossier ouvert au SGR ne relevait pas de la compétence du Comité R.

2.2. Consultation du dossier au SGR

Le Service d'enquêtes a pris connaissance des éléments contenus dans le dossier de l'intéressé existant au SGR.

Il est utile de préciser que Monsieur Y n'est pas militaire de carrière et qu'un certificat de sécurité lui a été délivré à l'occasion de ses activités d'officier de réserve.

En 1974, il a été affecté à un poste exigeant l'accès à des documents classifiés "TRES SECRET". Il a bénéficié d'un certificat de sécurité correspondant.

En 1975, Monsieur Y s'est rendu dans un pays de l'ancien bloc de l'Est pour des raisons privées.

Fin 1975, le SDRA (actuellement dénommé SGR/S, service de sécurité du SGR) a discuté de ce voyage avec Monsieur Y. Le SDRA a considéré que le plaignant était devenu une cible potentielle pour les services spéciaux du pays visité. Le dossier de Monsieur Y fait mention de cette prise de position du SDRA.

En 1977, la demande d'un certificat de sécurité "TRES SECRET" reçoit pour la première fois un avis négatif du SDRA. Cette décision n'est pas motivée, ce qui n'est pas particulier au cas de l'intéressé.

A partir de 1979, plusieurs documents du dossier du plaignant, font état des problèmes posés par la non-délivrance d'un certificat de sécurité à l'intéressé et par l'affectation de ce dernier à une fonction ne nécessitant plus un certificat de sécurité.

L'intéressé a entrepris de très nombreuses démarches auprès des autorités militaires et civiles afin d'obtenir un nouveau certificat de sécurité.

Finalement, le 6 mai 1982, le SDRA lui a accordé un certificat de sécurité du niveau "SECRET" valable jusqu'à la fin de ses obligations militaires, soit jusqu'au 31 décembre 1983.

3. CONSTATATIONS

Il a été impossible de déterminer la date précise à laquelle l'intéressé a signé la demande de renouvellement de certificat de sécurité, soit avant ou après son voyage dans un pays de l'ancien bloc de l'Est.

Des circonstances de la cause, le SDRA a estimé que l'intéressé était devenu une cible potentielle des services de renseignements d'un pays de l'ancien bloc de l'Est; nous sommes en 1975, la guerre froide n'est pas finie et l'intéressé est responsable d'un bataillon de réserve.

Selon le responsable actuel de la section chargée du traitement des enquêtes de sécurité, ces éléments auraient pu influencer le non renouvellement du certificat de sécurité de l'intéressé.

Une note de 1979 émanant du responsable des Forces de l'Intérieur rappelle qu'il est interdit de dévoiler à quiconque les motifs précis d'un refus d'octroi d'un certificat de sécurité.

Il ressort de l'analyse du dossier que la personnalité, les opinions et les fréquentations du plaignant ont fait l'objet de diverses hypothèses de la part du SDRA.

Dans le cas d'espèce, comme dans l'enquête relative aux certificats de sécurité⁽¹⁶⁾, le Comité R constate que le refus de renouvellement de certificat de sécurité n'a pas été formellement motivé. Il n'est dès lors pas possible de déterminer dans quelle mesure cette décision repose sur des faits avérés ou sur des supputations quant à la personnalité de l'intéressé.

4. CONCLUSIONS

1. L'exécution des enquêtes de sécurité et la délivrance des certificats de sécurité ne sont toujours pas réglées par une loi.
2. Le plaignant a complété et signé un formulaire de demande de certificat de sécurité. Il n'a pas été tenu au courant des modalités de l'enquête.
3. De par son voyage dans un pays de l'ancien bloc de l'est, il a dès lors été considéré comme une cible potentielle pour les services de renseignements de ce pays. Cet élément a pu influencer le non-renouvellement du certificat de sécurité de l'intéressé.
4. La manière dont l'enquête a été menée sur le terrain a donné lieu au recueil d'informations quant à la personnalité et aux opinions de l'intéressé.
5. Les critères dont il a été tenu compte dans la décision de ne pas renouveler le certificat de sécurité du plaignant ne sont cependant pas clairement établis.
6. A l'époque, il n'existait aucune prescription légale concernant l'accès à certains fichiers.
7. Monsieur Y n'a bénéficié d'aucune possibilité d'appel contre la décision de refus ou de retrait du certificat de sécurité.
8. La lecture du dossier fait apparaître que, fin des années '70, le plaignant a été mis au courant d'une partie des motifs du non-renouvellement de son certificat de sécurité. Il s'agit d'une faute individuelle commise par un membre du SDRA, contraire aux directives en la matière.

⁽¹⁶⁾ Rapport annuel d'activités du Comité R 1995, p. 125

Seul un recours aux cours et tribunaux compétents aurait pu offrir à l'intéressé la possibilité d'obtenir de l'Etat belge la communication du motif précis invoqué pour lui refuser la délivrance d'un certificat de sécurité ⁽¹⁷⁾.

9. Le non-renouvellement de son certificat de sécurité n'a pas empêché le plaignant de pouvoir exercer ses rappels en qualité d'officier de réserve, même si un changement d'affectation, décidé par l'armée, est intervenu. Le plaignant n'a pas subi de préjudice matériel.

5. RECOMMANDATION

Le Comité R recommande, à nouveau, que des dispositions légales relatives à la délivrance des certificats de sécurité et au recours éventuel des personnes concernées en cas de refus ou de suspension soient prises. Il est impératif que la Belgique respecte la jurisprudence de la Cour Européenne des droits de l'homme. Le Comité R n'ignore pas qu'un projet de loi est en cours d'élaboration en ce qui concerne cette problématique. Il se réjouit de cette initiative du gouvernement.

⁽¹⁷⁾ Rapport annuel d'activités du Comité R 1995, p. 133

TITRE II : NOS SERVICES DE RENSEIGNEMENT

DEUXIEME PARTIE : LES ENQUÊTES

D. ENQUETE COMMUNE DES COMITES P ET R
--

ENQUÊTE COMMUNE RELATIVE A LA DESTRUCTION EVENTUELLE DE DOCUMENTS PROVENANT DE LA POLICE JUDICIAIRE PAR LE SERVICE GENERAL DE RENSEIGNEMENT ET DE LA SECURITE (SGR)

1. INTRODUCTION

Le 27 mars 1996, un article signé par Walter De Bock dans le journal "De Morgen" causait un grand émoi dans le monde politique. L'article titrait : «De verdwijntruik van Generaal Georis».

Cet article mentionnait :

Militaire spionnen legden de hand op 'Terrorisme'-archief van de Brusselse Gerechtelijke Politie.

(...) De Militaire Geheime Dienst is er eind vorig jaar in geslaagd op illegale wijze de hand te leggen op het volledig archief van de Brusselse Gerechtelijke Politie over de 'Cellules Communistes Combattantes' (CCC), en andere gerechtelijke dossiers over terrorisme in België in de jaren '80.

In die periode werd bij de Gerechtelijke Politie in Brussel een aparte sectie opgericht, 'Groupe Répression du Terrorisme' (GRT), (...) in de loop van het gerechtelijk onderzoek naar de terreurgroep 'CCC', en ook nog jaren nadien, werd over dit onderwerp een goed gedocumenteerd archief samengesteld.

(...) De 'Groupe Répression du Terrorisme' werkte toen nauw samen met de Veiligheid van de Staat en de toenmalige Militaire Veiligheid wat de politieke inlichtingen betrof.

In het begin van de jaren '90 werd de Groupe Répression du Terrorisme (...)

De archieven bleven in kasten opgeslagen in een lokaal dat toebehoorde aan de Sectie Moord van de Brusselse Gerechtelijke Politie (...).

Op een dag in november 1995 (...) kwamen militairen het archief ophalen in de kantoren van de Gerechtelijke Politie Brussel (...) en verdween heel het Terrorisme-archief richting gebouwen van de Generale Staf in Evere".

Le journal indiquait également que les faits n'avaient été révélés que bien plus tard, c'est-à-dire au moment où le chef de la Police judiciaire bruxelloise a avoué à ses supérieurs qu'il avait remis les archives à la Sécurité militaire, parce que ce service disposait d'une broyeuse pour papiers alors que le sien n'en avait pas. Selon ses dires, ces documents devaient quitter rapidement les lieux en raison du manque de place.

Le lendemain, de nombreux journaux se faisaient l'écho de cette nouvelle. C'est ainsi que "Het Nieuwsblad" titrait "Deel Terrorisme-dossier vernietigd uit besparingsoverwegingen".

"De Gazet van Antwerpen" écrivait, pour sa part : "Gerechtelijk CCC-archief vernietigd ?".

Et la presse francophone n'était pas en reste. Pour preuve, le titre du journal "Le Soir" :

«Surréalisme : le Renseignement militaire nettoie les armoires de la Police Judiciaire de Bruxelles. CCC : les archives offertes au SGR».

Cet article d'Alain Guillaume faisait également référence à la question parlementaire que le Sénateur Boutmans (Agalev) avait adressée aux ministres de la Défense nationale et de la Justice sur ce sujet.

2. PROCEDURE

A la suite de l'article paru dans le journal "De Morgen" du 27 mars 1996, le Président du Comité P a proposé au Comité R, dans une lettre datée du 28 mars 1996, de mener une réunion commune.

Au cours de la réunion commune des comités P et R, le 1^{er} avril 1996, il a été décidé de procéder à cette enquête.

Un membre du Comité P et un membre du Comité R ont reçu pour mission de suivre et de contrôler cette enquête, et de rendre régulièrement compte aux Comités du déroulement de celle-ci.

Une équipe mixte d'enquêteurs a ainsi été constituée, placée sous la direction du chef du Service d'enquêtes du Comité P.

Par lettre du 5 avril 1996, les Présidents de la Chambre et du Sénat ont été informés, conformément à l'article 46, troisième alinéa, du règlement d'ordre intérieur, qu'une enquête de contrôle avait été ouverte.

Entre le 1^{er} avril et le 5 novembre 1996, l'équipe mixte d'enquêteurs a reçu diverses missions.

Par lettre du 16 avril 1996, le Procureur général de Bruxelles a informé le Président du Comité P qu'aucune enquête judiciaire ou information n'était en cours dans son ressort au sujet du transfert d'une partie des archives de la Brigade de police judiciaire de Bruxelles au Service de Sécurité de l'Armée.

Le 10 mai 1996, l'Inspecteur général de la Police judiciaire signala par écrit au Comité P que son service ne menait aucune enquête à cet égard.

Interrogé sur les motifs de cette absence d'enquête, il répondit le 17 juin 1997, qu'il n'en avait pas été chargé par un de ses supérieurs et que, après concertation avec le Comité P, il est apparu que les Comités P et R s'en chargeraient.

En outre, il est d'avis qu'il s'agit de la meilleure solution, car son service n'est pas compétent pour les membres du personnel des services qui ne dépendent pas de la Police judiciaire.

Le 22 avril 1996, les ministres de la Défense nationale et de la Justice ont été informés par le chef du Service d'enquêtes P, conformément à l'article 43, alinéa 1 de la loi du 18 juillet 1991 organique du contrôle des Services de police et de renseignements, qu'une enquête de contrôle avait été ouverte.

3. ORIGINE DE L'ENQUÊTE

Le 11 janvier 1996, le Sénateur Boutmans (Agalev) a adressé une question aux ministres de la Justice et de la Défense nationale (Questions n° 89 et 17 - Questions et Réponses - Sénat - 12 mars 1996 et 13 février 1996) :

«Retrait de documents à la Police judiciaire par le Service de Sécurité militaire.

J'apprends que des agents du Service de Sécurité Militaire, ou du moins des personnes qui se sont présentées en cette qualité, se sont rendus à la Police Judiciaire de Bruxelles fin novembre ou début décembre 1995, pour y réclamer un certain nombre de documents relatifs aux CCC et à la Bande de Nivelles.

Pouvez-vous confirmer cette information ? Si elle est exacte, en vertu de quelle compétence et à quelle fin, le Service de Sécurité militaire a-t-il agi de la sorte ?

(...) S'agissait-il de documents qui relevaient du devoir de discrétion à l'égard des enquêtes judiciaires ? La Sécurité militaire mène-t-elle sa propre enquête et si oui, sous la responsabilité de qui ? »

Le ministre de la Défense nationale a répondu comme suit :

- « 1. Il est inexact d'affirmer que du personnel du Service général du renseignement et de la sécurité aurait réclamé auprès de la police judiciaire de Bruxelles des documents ayants traits aux CCC et à la bande de Nivelles.*
- 2. Des membres du personnel du commissariat général de la police judiciaire de Bruxelles, confrontés au problème de la destruction de pièces non judiciaires qui ne présentaient plus aucun intérêt pour les enquêteurs, ont par contre pris contact, fin 1995, avec le Service général du renseignement et de la sécurité. Leur souci était d'éviter les coûts de destruction de ces documents par une firme privée.*
- 3. Tous les documents transmis ont été détruits par les soins du Service général du renseignement et de la Sécurité».*

(Questions et Réponses - Sénat - 13 février 1996 (n° 1-10)).

Dans le journal "Le Soir" du 29 mars 1996 est paru l'article suivant :

«Le porte-parole du Parquet de Bruxelles a répondu, hier, aux révélations du quotidien «De Morgen» relatives au "cadeau" (les archives de la Police Judiciaire sur le terrorisme européen dans les années 80) offert par le patron de la Police Judiciaire de Bruxelles aux espions du Service général de renseignement de l'armée.

Selon le Parquet, ces papiers ne concernaient que des coupures de presse inutiles et inexploitable. Elles n'avaient aucun caractère judiciaire. Avant destruction eut lieu un tri scrupuleux effectué par la section crime.

Dont acte... mais alors pourquoi fallait-il absolument passer ces "coupures de journaux" à la broyeuse de documents ? » (signé Alain Guillaume).

Dans son édition du 29 mars 1996, "De Morgen" abordait cette affaire dans un autre article, en titrant : "Steeds meer vragen over verdwijning Gerechtelijke Politie - archief".

Le journal soulignait que la manière dont le "Service d'espionnage militaire" est intervenu, continuait à soulever de nombreuses interrogations dans le monde policier.

La question principale porterait sur la manière dont ces archives ont pu disparaître. D'un point de vue légal, les archives policières des Brigades de police judiciaire près les Parquets appartiennent au Parquet général.

Le quotidien ajoute que le Commissaire en chef faisant fonction de la Police judiciaire bruxelloise, qui, de sa propre initiative, a pris la décision de remettre les archives, essayait de se tirer d'affaire en déclarant qu'il ne s'agissait que de documents non judiciaires, dont des coupures de presse.

Le journaliste (Walter De Bock) conclut :

«Kortom, in deze zaak werden om één of andere duistere redenen systematisch alle bevoegde autoriteiten en diensten (de Rijksarchieven, het Parket en de AGG (Anti-Terroristische Gemengde Groep) omzeild ".

Il est apparu, tant de la question du Sénateur Boutmans que des déclarations du porte-parole du Parquet de Bruxelles, qu'au moins une partie de la documentation de la section "Groupe de Répression du Terrorisme" de la Police judiciaire de Bruxelles avait été transmise au SGR.

Les Comités P et R ont donc ouvert l'enquête de contrôle dans le but de vérifier quelles étaient les pièces la Police judiciaire de Bruxelles qui avaient été transférées au SGR, dans quelles circonstances et pour quelles raisons.

En effet, ces articles et cette question parlementaire mettaient autant en cause la crédibilité de la Police judiciaire bruxelloise que celle du SGR.

Le but de cette enquête est de vérifier si, dans le cadre des faits cités, des dysfonctionnements sont apparus et, surtout, de formuler des recommandations pour améliorer le fonctionnement du service de police ou de renseignement concerné.

En outre, les Comités P et R ont voulu s'assurer que cette manière d'agir ne violait pas les droits que la Constitution et les lois confèrent aux particuliers.

4. SYNTHÈSE DE L'ENQUÊTE

4.1. Contexte de la problématique

L'article 39 de la loi du 5 août sur les fonctions de police prévoit :

"Dans l'exercice des missions qui leur sont confiées, les services de police peuvent recueillir des informations, traiter des données à caractère personnel et tenir à jour une documentation relative notamment à des événements, à des groupements et à des personnes présentant un intérêt concret pour l'exécution de leurs missions de police administrative ou judiciaire.

Les renseignements contenus dans la documentation doivent présenter un lien direct avec la finalité du fichier et se limiter aux exigences qui en découlent.

Ces renseignements ne peuvent être communiqués qu'aux autorités et services de police ainsi qu'aux services de renseignement officiels qui en ont besoin pour l'exécution de leurs missions".

Fin octobre 1984, la Police judiciaire bruxelloise a constitué le "Groupe de Répression du Terrorisme" (GRT), à la demande du Parquet de Bruxelles, après les premiers attentats des CCC.

Cette cellule d'enquête a constitué une documentation sur les personnes suspectées d'entretenir des liens avec les CCC.

La base de la documentation se composait de différents dossiers et fiches de la Section Centrale de la police judiciaire, chargée des enquêtes politiques, comme celles qui visaient le Front de la Jeunesse et les différents attentats à la bombe.

Dans un deuxième temps, on y ajouta les éléments de l'opération "MAMMOUTH", soit le résultat d'une centaine de perquisitions.

Cette documentation a été complétée par des rapports de la Sûreté de l'Etat et des copies de procès-verbaux, établis à l'occasion des réunions de travail conjointes et transmis par la Gendarmerie ou par le Juge d'instruction Lyna.

Le "Groupe de Répression du Terrorisme" n'a jamais été dissout officiellement. Mais les membres de la cellule ont été intégrés dans la Section crime.

Au cours de l'enquête de contrôle, le Chef du "Groupe de Répression du Terrorisme" de l'époque a constaté qu'un grand nombre de pièces avaient été retirées de la documentation (déplacées ou détruites).

Ainsi, ont notamment disparu :

- tous les dossiers «Associations»;
- les dossiers «Espionnage»;
- les dossiers individuels;
- les dossiers «Attentats sur les universités»;
- les dossiers d'enquête «Parti du Travail» et «Nouvelle Acropole».

Dans un grand nombre de ces dossiers se trouvaient des copies de procès-verbaux.

Il manquait également :

- des centaines de copies de procès-verbaux;
- certains rapports du service de déminage;
- des radiogrammes d'Interpol ;
- des rapports "Danger-Source" de la Sûreté de l'Etat ;
- des rapports de surveillance ;
- des rapports contenant des données recueillies par « Zoller-Malicieux ».

De plus, il est apparu que différents autres dossiers ne figuraient plus dans la documentation, mais que ceux-ci, dispersés dans la brigade, ont été conservés par d'autres membres de la police judiciaire de Bruxelles".

L'ancien chef du "Groupe de Répression du Terrorisme" a déclaré que, du fait que la documentation conservée dans son service comportait une grande quantité de procès-verbaux et de rapports confidentiels au moment de son départ en 1994, seul un magistrat pouvait donner l'autorisation de transférer les documents.

Etant donné que les membres du SGR ne jouissent pas de la qualité d'officier de police judiciaire, il est exclu, selon lui, que la décision de procéder au transfert ait été prise par un membre de la police judiciaire.

Pour cette raison, il a informé le Magistrat national du transfert.

Il a ajouté que, selon lui, le "Groupe de Répression du Terrorisme" n'a pas collaboré efficacement et officiellement avec le SGR.

4.2. Le déroulement de l'enquête de contrôle

4.2.1. La première phase

A) Les faits

L'enquête a pu déterminer qu'une grande partie de la documentation du "Groupe de Répression du Terrorisme" a été transférée au SGR le 30 novembre 1995.

Etant donné que tout a été détruit (en admettant que les choses se soient déroulées de cette manière), il n'a pas été possible de déterminer ce qui a été réellement déménagé.

Cependant, il est clair que la demande de transfert venait du Commissaire Principal de Première Classe de la Police judiciaire de Bruxelles, Chef du service.

C'est bien ce dernier qui a donné l'ordre de trier la documentation. Il a affirmé ignorer le contenu et la valeur de la documentation, que cette dernière n'était plus d'actualité et que le SGR n'y trouverait certainement rien de nouveau.

Toutefois, l'enquête a fait apparaître que certaines caisses ont été marquées d'un 'D' pour 'Destroy' au cours du déménagement, car elles contenaient des pièces manifestement inutiles (des annuaires téléphoniques, par exemple).

Selon le degré de responsabilité (chefs et subalternes), il ressort de certaines déclarations que la documentation contenait des documents utiles (notamment une documentation sur la RAF (Rote Armee Fraktion), sur la PIRA (Provisional Irish Republican Army) et des dossiers (individuels), ainsi que des copies de procès-verbaux.

Plusieurs caisses non marquées, contenant des papiers, ont d'abord été conservées, aux fins d'examen, dans un département civil du SGR.

De l'enquête interne au SGR menée le 29 mars 1996, les éléments suivants sont apparus :

Le déménagement de ± 3 à 4 m^3 de dossiers de la police judiciaire de Bruxelles vers le SGR/CI (Cellule Subversion & Terrorisme) a été effectué le 30 novembre 1995 avec un véhicule de l'armée.

Après un premier tri, les spécialistes du SGR/CI ont procédé à une vérification.

Les documents qui leur paraissaient importants ont été synthétisés dans des rapports et ont été ensuite détruits à la broyeuse (entre le 30 novembre et la mi-décembre 1995).

Dans un deuxième temps (de la mi-décembre 1995 à la mi-janvier 1996), des documents ont été transférés, par manque de place, à une adresse privée. Une partie de ces documents a ensuite été récupérée pour examen.

Dès qu'elle a eu connaissance de la présence des pièces, la direction du SGR a donné l'ordre exprès de tout détruire sur-le-champ.

Dans un troisième temps (du 14 au 18 janvier 1996), tout a été détruit, à l'exception de trois dossiers et des fiches manuscrites.

Le 27 janvier 1996, trois dossiers ont encore été détruits.

Au cours de l'enquête interne, il a été constaté qu'un membre du SGR/CI n'a pas donné suite à l'ordre formel du SGR/S. Après son audition, il s'est exécuté et tous les documents restants de la police judiciaire ont été détruits.

B. Les questions soulevées par l'enquête :

1. Quelle est l'importance de la documentation ?

Selon deux officiers de la Police judiciaire responsables, la documentation du "Groupe de Répression du Terrorisme" n'était pas importante. Cependant, il ressort de leurs déclarations qu'ils ne connaissaient pas le contenu de la documentation.

D'autre part, la documentation a été examinée et, pendant le déménagement, une partie a été placée dans des caisses marquées de la lettre 'D' (pour 'Destroy'). Or, il s'avère qu'au fil du temps, plusieurs dossiers ont été extraits de la documentation et conservés en différents endroits de la brigade de la police judiciaire.

Pour le SGR aussi, la documentation devait présenter quelque intérêt, En tout cas, on n'a pas procédé immédiatement à sa destruction et les documents ont été examinés autant que possible. Un membre du SGR a déclaré que la documentation contenait des informations utiles et qu'elle lui aurait permis de compléter la documentation disponible dans son service.

Il a été impossible, du fait de leur destruction, d'évaluer la valeur réelle des documents.

Cependant, l'enquête a montré qu'un magistrat du Parquet de Bruxelles manifestait encore de l'intérêt pour le dossier des CCC.

Le 9 décembre 1994, un substitut du Procureur du Roi avait requis instruction sur l'éventuelle infiltration des CCC.

Le 21 septembre 1995, ce dossier a été transmis au Procureur du Roi par le juge d'instruction pour réquisitions.

Le réquisitoire de non-lieu du Procureur du Roi date du 14 décembre 1995.

Cette enquête judiciaire a été clôturée par une ordonnance de la Chambre du conseil du 21 décembre 1995 concluant à un non-lieu.

Mais cette décision n'a pas mis un terme à l'information en cours au Parquet.

Un commissaire de la police judiciaire de Bruxelles consultait encore régulièrement la documentation du Groupe de Répression du Terrorisme et rédigeait, sur ce sujet, des rapports confidentiels à destination du Parquet.

Cet officier de police déclarait :

"S'il devait apparaître que cette documentation a été détruite, elle ne pourra plus être reconstituée. Il s'agit d'une véritable perte."

Il est également ressorti de sa déclaration que le dossier de CCC restait encore ouvert contre X chez un juge d'instruction.

L'enquête a également fait apparaître que le même magistrat du Parquet avait confié au Service d'enquêtes du Comité R, en octobre 1995, une mission relative aux CCC.

Cette mission n'a pas été exécutée, car le chef du Service d'enquêtes du Comité R fit remarquer que l'article 51 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements n'était pas applicable en l'espèce.

Le chef du Service d'enquêtes demanda des instructions, à cet égard, au Procureur du Roi de Bruxelles.

Après un entretien téléphonique avec le Procureur du Roi, la mission non-exécutée a cependant été renvoyée à ce magistrat, le 9 novembre 1995.

Le dossier relatif à l'enquête judiciaire clôturée a été réclamé au Procureur général de Bruxelles. Le Procureur général fit savoir que le dossier avait été transmis au ministre de la Justice dans le cadre d'une procédure disciplinaire à l'encontre d'un magistrat.

Le dossier a ensuite été transmis aux Comités P et R.

Une source potentielle d'informations a ainsi été soustraite à l'enquête judiciaire par la destruction des dossiers.

2. Qui a donné l'ordre de transférer la documentation ?

Bien que le Commissaire principal faisant fonction en ait assumé l'entière responsabilité, il est évident que la décision effective incombait au Chef du service.

Au SGR, les accords de transfert ont été conclus par une autorité civile d'un échelon inférieur du service. La section concernée n'a pas établi de rapport à ce sujet. A l'origine, la direction militaire

n'était pas au courant. Dès qu'elle en a été informée, elle a donné l'ordre exprès de détruire la documentation.

3. Pour quelle raison la documentation a-t-elle été transférée ?

C'était peut-être la question essentielle.

Selon les officiers de la police judiciaire responsables, le transfert se justifiait par un manque de place et par le caractère insignifiant des documents. Dans le rapport d'enquête interne du SGR, le but recherché est décrit de manière plus nuancée.

Pour la police judiciaire, il s'agissait de faire le nettoyage et de rendre un service au SGR.

Pour le SGR, l'objectif était d'exploiter la documentation et de rendre le service demandé (destruction)⁽¹⁾.

4. La manière dont la documentation sur le Groupe Répression du Terrorisme a été traitée et les directives y relatives :

Pour la Police judiciaire

Le Commissaire général a été interrogé à de multiples reprises sur le contenu des directives en vigueur en matière d'archivage et de destruction.

Le Directeur des Archives du Royaume a également adressé une question au Commissaire général à la suite de l'article paru dans "De Morgen ".

A cet égard, il a été fait référence à l'autorisation préalable du Parquet et du Directeur des Archives du Royaume lui-même. La police judiciaire a répondu qu'il n'existait aucune directive et que cette matière faisait l'objet d'une concertation avec le Directeur des Archives du Royaume.

Il ressort d'une lettre du 9 janvier 1997 qu'une étude est en cours en ce qui concerne la documentation, tant au Commissariat général de la Police judiciaire que dans les brigades.

Une fois que cette étude sera terminée, des directives seront communiquées.

De plus, on signale que le ministère de la Justice prépare des directives relatives à la prescription des délits, au secret professionnel et à la protection de la vie privée.

Il a vraisemblablement échappé à l'attention de la direction de la Brigade de la Police judiciaire de Bruxelles qu'il existe, le GIA (le Groupe Interforces Anti-Terroriste), spécifiquement chargé du domaine auquel se rapporte la documentation transférée et détruite du "Groupe de Répression du Terrorisme".

Le responsable de ce service déclare qu'il n'a pas été contacté et que son service adopte une autre méthode de travail : son service prend d'abord contact avec l'organisme qui a émis les documents si ces derniers sont confidentiels. Un membre du GIA reste présent en cas de destruction par le SGR.

⁽¹⁾ Traduction libre

Pour le SGR

En ce qui concerne la destruction des documents classifiés, le SGR dispose des directives reprises dans les "Ordres Généraux J/300 B" (Instructions relatives aux Archives de la Défense nationale) et l'OG J/397 D (Centre de documentation historique), ainsi que des directives de la Sécurité Territoriale, dont la DST 22 (Sécurité des Documents - Classement - Déclassement) et la DST 24 (Sécurité des Documents - Reproduction - Destruction), qui sont d'application pour l'ensemble des forces armées.

Ces ordres ne comportent donc aucune directive relative aux documents qui proviennent d'une instance non militaire.

En ce qui concerne les dossiers de la Contre-ingérence, à qui une partie de la documentation de la Police judiciaire a été remise, ils sont conservés et traités conformément aux directives de la section CI.

4.2.2. La deuxième phase

Suite à la mission du 12 mars 1997, une enquête a tenté de déterminer ce qui subsistait encore, à la police judiciaire, de la documentation du Groupe de Répression du Terrorisme; son contenu a été examiné et comparé avec les déclarations initiales.

Il apparaît, contrairement aux déclarations faites pendant la première phase, que la plupart des dossiers étaient encore bien présents au sein de la brigade de Bruxelles.

Cette nouvelle version, attestée au moyen d'une vérification, s'explique par le fait que, après le départ du responsable du Groupe de Répression du Terrorisme, la tenue et la conservation de la documentation ont laissé à désirer.

Le local et les armoires contenant la documentation restaient ouverts, de sorte que tout le monde avait librement accès à n'importe quel dossier.

Beaucoup de personnes en ont profité pour transférer une partie de la documentation dans d'autres locaux ou d'autres services. Etant donné qu'il n'existait aucun registre de prêt, ces déplacements pouvaient s'opérer sans que cela ne se remarque.

Les dossiers ainsi empruntés n'étaient pas remis en place par manque de contrôle et d'inventaire.

Dans la première phase, on n'avait pas évoqué la possibilité que les principaux dossiers puissent se trouver ailleurs dans la brigade.

Il n'empêche qu'une grande quantité de documentation a été transférée au SGR et qu'ainsi, des documents confidentiels et des copies de procès-verbaux ont été déménagés.

Les 10 et 12 juin 1997, les présidents des Comités P et R ont reçu, de la part du Commissaire général, des lettres avec annexes, contenant des missions judiciaires.

Après consultation des pièces, on peut présenter schématiquement la problématique relative à la gestion des archives comme suit :

- On a trouvé deux notes, relatives à ce sujet, au Parquet général de Bruxelles : une lettre datée du 18 février 1958 et une autre du 13 août 1996, contenant des instructions du Secrétaire général du département de la Justice pour la gestion des archives.

Selon le Commissaire général, ces notes, bien qu'elles soient importantes pour la police judiciaire, n'ont jamais été transmises à la direction de la police judiciaire. Leurs seuls destinataires furent les greffiers en chef et les secrétaires de parquet. Le chef du service de documentation du Parquet de Bruxelles pense qu'elles n'ont pas été transmises à la police judiciaire parce qu'elles ne concernaient que les archives des Tribunaux.

- En 1981 et en 1983, le Commissaire général de l'époque donna des instructions pour la gestion de la documentation; mais celles-ci ne s'appliquaient qu'au personnel du Commissariat général.
- Le 25 avril 1989, son successeur donna également des instructions pour la gestion de la documentation, uniquement valables une fois encore pour le Commissariat général.
La personne chargée de la gestion de la documentation du Commissariat général a soumis au Commissaire général, le 15 mars 1993, un projet de note, destiné à l'Archiviste général du Royaume. Cette note porte sur les autorisations nécessaires pour détruire, principalement, les "doublons", car on constate un manque évident d'espace de stockage. Selon la personne responsable de la documentation, ladite note n'a jamais été signée par le Commissaire général et, par conséquent, n'a jamais été expédiée.
Pendant cette période, des contacts ont bien eu lieu entre le Commissaire général et l'Archiviste général du Royaume, notamment les 8 et 12 juillet 1993. Ces discussions n'ont donné aucun résultat.
- Le 24 octobre 1994, un entretien a eu lieu entre la personne chargée de la gestion de la documentation du Commissariat général et un représentant des Archives générales du Royaume. A la suite de cette entrevue, ce dernier a rédigé un rapport interne.
Cependant, le Commissariat général et les brigades de la police judiciaire n'ont formulé aucune proposition à propos de la gestion des archives.
- Après la parution d'articles dans la presse au sujet de la destruction des archives du GRT, le Commissaire général et l'Archiviste général adjoint ont repris contact. Le point de vue de ce dernier revient à dire qu'il faut respecter scrupuleusement le texte de la loi du 24 juin 1955 relative aux archives.
- Le Commissariat général a rédigé des instructions provisoires uniquement à l'attention des services du Commissariat général.

Le comité de direction doit décider si ces instructions peuvent aussi s'appliquer aux brigades.

Les Archives générales du Royaume adoptent une attitude attentiste à l'égard de ces instructions provisoires, car ce service souhaite d'abord terminer son enquête au sein de la police judiciaire.

5. CONSTATATIONS

5.1. En ce qui concerne la Police judiciaire

- Le Groupe de Répression du Terrorisme n'a jamais été officiellement dissout. Les membres de ce groupe ont été intégrés à la Section crime.
- Après le départ du responsable du Groupe Répression du Terrorisme, la tenue et la conservation de la documentation ont laissé à désirer. Le local et les armoires contenant la documentation restaient ouverts, de sorte que tout le monde pouvait avoir librement accès à n'importe quel dossier.

Certains membres ont récupéré une partie de la documentation qui a été conservée à d'autres endroits.

Etant donné qu'il n'existait aucun registre de prêt, il n'a pas été et il n'est toujours pas possible d'en retrouver la trace.

- Cette enquête de contrôle a montré que cette méthode de travail entraîne une forte concentration de l'expérience et des connaissances parmi certains membres de la police judiciaire de Bruxelles, ce qui peut exercer une influence néfaste sur la cohésion et le bon fonctionnement de l'ensemble de ce service de police. Ce problème fera éventuellement l'objet d'une enquête de contrôle par le Comité P.
- Les responsables de la brigade de Bruxelles ont soutenu qu'il s'agissait d'une documentation peu importante et inutile. L'enquête de contrôle a cependant révélé qu'ils manifestaient peu d'intérêt pour le contenu et la valeur de cette documentation et qu'ils en avaient une faible connaissance.
- Bien que le Commissaire en chef faisant fonction en ait assumé toute la responsabilité, il était manifeste que la décision avait été prise, en réalité, par le Chef du service.
- Bien que les pièces transférées pour destruction comprenaient de nombreuses copies de procès-verbaux, les autorités judiciaires n'ont pas été informées au préalable de ce transfert ni sollicitées pour approbation.
- Personne n'a tenté d'entrer en contact avec le responsable du GIA, alors que ce service est chargé de la tenue et de l'étude de la documentation relative au terrorisme. Aucun contact n'a davantage été pris avec d'autres instances telles que la Sûreté de l'Etat, alors que la documentation comprenait des rapports émanant de ce service et portaient la mention "Danger-Source". Une enquête distincte sera ouverte par le Comité R, entre autres sur la manière dont ces documents ont été traités.
- En matière de destruction de documents, la Police judiciaire devait tenir compte de la loi du 24 juin 1955 relative aux archives ainsi que de l'arrêté royal d'exécution du 12 décembre 1957.

L'article 1^{er} de la loi stipule :

"Les documents datant de plus de cent ans conservés par les tribunaux de l'ordre judiciaire, le Conseil d'Etat, les administrations de l'Etat et les provinces sont déposés - sauf dispense régulièrement accordée - aux Archives de l'Etat."

Et l'article 5 :

"Les autorités visées à l'article 1^{er}, alinéas 1 et 2, ne pourront procéder à la destruction de documents sans avoir obtenu l'autorisation de l'Archiviste général du Royaume ou de ses délégués."

Ce qui n'a pas été fait en l'espèce.

- Les seuls contacts établis entre le Commissariat général et les Archives du Royaume, au sujet des faits du 30 novembre 1995, n'ont livré aucun résultat tangible.
- Hormis la loi sur les archives, la police judiciaire ne dispose d'aucune procédure ou directive pour l'archivage ou pour la destruction de pièces.
Au fil du temps, quelques instructions ont bien été données pour la gestion de la documentation, mais celles-ci ne concernaient que le Commissariat général.
- En détruisant ces dossiers, une source potentielle d'informations a ainsi échappé aux informations menées par le parquet et aux instructions judiciaires.
L'enquête de contrôle a révélé qu'au moment du déménagement de la documentation de la police judiciaire de Bruxelles au SGR, différentes enquêtes judiciaires étaient encore pendantes, à savoir :
 - a) l'infiltration éventuelle des CCC, à laquelle la Chambre du conseil n'a mis fin que le 21 décembre 1995 en prononçant un non-lieu;
 - b) l'assassinat de Bull (enquête toujours en cours);
 - c) l'instruction judiciaire sur les CCC, ouverte contre X, n'est pas encore clôturée;

De plus, certaines déclarations indiquent que plusieurs enquêtes d'information du parquet utilisant cette documentation sont encore en cours. Un membre de la Police judiciaire se réfère à la mission qui lui a été confiée en 1997 par un des magistrats nationaux à propos d'un attentat terroriste qui remonte à dix ans. Il a confirmé qu'il pouvait satisfaire à cette demande.

- A la suite de ces faits, aucune enquête interne n'a été menée au sein de la police judiciaire.

5.2. En ce qui concerne le SGR

Une enquête interne menée au SGR a permis de tirer les leçons suivantes :

1. Le Commandement n'avait pas été préalablement informé d'une opération importante.
2. L'indépendance excessive dans l'étude des documents par le C/Subversion, malgré des directives claires données par le CI (contre-ingérence), lequel avait toutefois pris la responsabilité de l'opération.
3. La non-exécution par le C/Subversion (en particulier par X) des directives données par le CI en matière de destruction⁽²⁾.

⁽²⁾ Traduction libre

Les deux Comités peuvent s'y associer.

L'acceptation de la documentation de la Police judiciaire ne peut être reprochée au SGR.

Il ressort de la note du GIA n° 548/21-68 du 23 septembre 1990 - Secret (cette note générale contient la répartition des objectifs et elle est signée par le Directeur du GIA), que le SGR participait dans le passé - et participe encore - aux mesures de prévention contre le terrorisme. Le SGR est représenté en permanence au GIA.

Les auditions menées au SGR permettent de conclure qu'il n'était plus possible de déterminer quelles étaient les informations provenant de la documentation de la Police judiciaire.

Cette problématique sera traitée ultérieurement par le Comité R, car elle ne concerne que les services de renseignement.

Aucun dysfonctionnement n'a été constaté au SGR, ni à propos de l'efficacité du service, ni à l'égard du respect des droits que la Constitution et la loi confèrent aux citoyens.

6. RECOMMANDATIONS A L'EGARD DE LA POLICE JUDICIAIRE

Des directives sur la manière dont les informations doivent être conservées, traitées et mises à disposition doivent être établies.

Il faut également prévoir une procédure de destruction.

La méthode utilisée par le Groupe Interforces Anti-Terroriste (GIA) peut servir d'exemple.

Selon une note interne du 5 juin 1997, le Commissariat général mène actuellement une concertation permanente avec les Archives du Royaume afin d'établir des instructions pour la gestion de la documentation.

Le personnel des Archives du Royaume s'est informé auprès des brigades sur la nature des documents qu'elles conservent.

Ces instructions doivent permettre de décider si un document

- doit être conservé dans le service;
- doit être conservé par les Archives du Royaume;
- ou s'il faut le détruire.

Ensuite, les instructions nécessaires doivent être élaborées réglant l'application des directives ci-dessus mentionnées, par les différentes brigades de la police judiciaire.

Le Comité de direction de la police judiciaire doit prendre une décision à ce sujet.

L'avis des Parquets généraux est indispensable, car il s'agit de documents sur lesquels ils ont un droit de regard.

Le résultat final de ces travaux est d'obtenir une instruction pour la gestion des archives des services de police.

Enfin, Il faudra veiller attentivement au respect des procédures et des prescriptions légales.

Il faudra également veiller à ce que le caractère judiciaire de certaines pièces ne disparaisse pas, même s'il s'agit de copies.

TITRE III : CONTACTS DU COMITE

CHAPITRE 1 : CONGRES DE WASHINGTON

Au cours du mois de septembre 1996, un membre du Comité R fut invité à participer à trois congrès à Washington.

Eu égard aux sujets abordés lors de ces congrès, le Comité R estima indiqué que ce membre y assiste.

Les thèmes suivants furent traités :

- INFOWARCON;
- OPEN SOURCES SOLUTIONS;
- LAW ENFORCEMENT AND INTELLIGENCE.

A. INFOWARCON

D'après Winn Schwartau⁽¹⁾, "Information Warfare" peut être définie comme suit :

"L'utilisation offensive ou défensive d'informations et/ou de systèmes d'informations dans un conflit."

Le Pentagone ajoute à cette définition :

"Dans le but, de corrompre ou de détruire les informations et/ou les systèmes d'informations de l'adversaire, mais aussi de protéger notre propre structure de l'information."⁽¹⁾

(1) Aux Etats-Unis, Winn Schwartau est l'un des experts directeurs dans le domaine de la protection de l'information. Il a témoigné devant des sous-commissions parlementaires et conseille aussi bien le monde de l'industrie que le gouvernement. Il est aussi un écrivain productif qui a publié des centaines d'articles dans des magazines tels que Computer World, Info World, PC Week, Network World et Info Security News.

(2) Traduction libre.

Les orateurs de ce congrès partent du principe que chaque citoyen est tôt ou tard victime de "l'Information Warfare".

Il est acquis que notre avenir et celui de nos enfants dépendront en grande partie de la façon dont nous aborderons la "Révolution de l'information" et les problèmes y afférents.

Partant de l'idée, que la protection de la vie privée est possible, que les données économiques et la sécurité nationale peuvent être préservées de façon efficace même si c'est difficile, ils ont essayé de trouver des réponses à ces questions : comment reconnaitrons-nous "l'Information Warfare" et comment la démocratie, les entreprises et les citoyens peuvent-ils s'en prémunir?

Les différentes interventions peuvent être résumées comme suit :

la guerre mondiale économique dans les pays industrialisés a débuté. Elle implique des intimidations et des agressions et vise l'infrastructure informative et financière de l'économie occidentale.

La société moderne et les entreprises se basent sur les connaissances, l'accès aux informations exactes et l'utilisation intensive de la technologie de la communication. Un ordinateur peut causer plus de dégâts à la vie économique et à la sécurité nationale que des armes conventionnelles

Les protagonistes du crime organisé pourraient exercer un chantage s'il réussissaient par exemple à désorganiser le trafic aérien, maritime ou ferroviaire; à entamer la protection des données économiques ou industrielles; à dérégler la circulation nationale et internationale de l'argent ou à rassembler des données concernant la vie privée. Un "Pearl Harbour" électronique n'est pas à exclure selon les Américains.

Le maintien de la sécurité est une mission de l'Etat. La protection des informations et de leurs systèmes en fait partie et est cruciale notamment pour la vie économique.

Ils doivent être protégés de manière efficace. Il ne suffit pas seulement de mettre les informations à l'abri du danger, mais il faut également sécuriser les moyens leur donnant accès.

"L'Information Warfare" fera partie intégrante du nouveau paysage politique et économique parce que l'information représente un pouvoir politique et économique.

Les données relatives à la vie privée sont rassemblées dans différents systèmes informatiques qui sont, pour la plupart, insuffisamment protégés des intrusions et des modifications malveillantes sans oublier qu'ils peuvent également contenir des données erronées. D'aucuns pourraient faire un usage abusif des informations sur notre solvabilité, sur des rapports médicaux, sur notre appartenance ou non à une organisation politique ou autre.

De nombreuses entreprises sont inconscientes du danger que représente l'espionnage économique et des conséquences liées à une intrusion dans leurs systèmes d'informations ou à une désorganisation de ceux-ci. Les cas de nombreuses entreprises "tuées par l'électronique" furent citées, précisément parce qu'elles étaient incapables d'identifier leur ennemi.

"L'ennemi est anonyme et invisible."

Les milieux bancaires ont connu de sérieux problèmes en raison de leur informatisation. Plusieurs exemples américains furent évoqués.

Ces difficultés ne sont pas uniquement provoquées par le "hacking", elles peuvent aussi être

attribuées à des erreurs ou à une manipulation du software et du hardware.

L'utilisation frauduleuse de l'informatique par des employés indécents a, à plusieurs reprises, causé un préjudice aux sociétés commerciales.

Il a été question d'une banque déclarée en faillite, notamment en raison d'un usage frauduleux de l'informatique (la banque Barrings).

Internet, nouveau "business", crée de nombreuses possibilités en ce qui concerne les nouveaux marchés entre autres. Les particuliers s'initient extrêmement vite à telle enseigne qu'ils utilisent déjà des e-mails à des fins commerciales. Mais cette technique comporte toutefois beaucoup de risques tant pour la vie privée que sur le plan matériel. Par exemple, lors d'une demande de carte de crédit, différentes étapes sont nécessaires avant que celle-ci ne parvienne à son destinataire. Le risque de fraude est donc très élevé.

Il est indéniable qu' Internet impose aux services de police et de renseignement un surcroît de travail parce qu'il leur faut combattre de nouvelles formes de criminalité. Ces services devront essayer d'anticiper les activités des criminels. Toutefois, Internet constitue pour ces services un nouvel outil de travail.

L'apparition de nouveaux moyens de télécommunication multiplie les possibilités de fraude . Les criminels voient leur champ d'action s'élargir. De ce fait, le travail des services de police et de renseignement s'accroît. De nouvelles techniques, utilisées comme moyens pour combattre cette forme spécifique de criminalité, naissent : il s'agit de terminaux de données mobiles, système de filature, d'analyse de réseau, de cryptographie sophistiquée, etc.

La manière d'envisager la protection de l'information a été modifiée. Il y a quelques années, la protection se limitait à constater un défaut auquel on remédiait. A l'heure actuelle, cette problématique est étudiée avant l'installation d'un système informatique.

En résumé, la façon d'aborder le problème de la protection de l'information doit évoluer. Les concepteurs doivent passer d'une approche réactive à une approche proactive.

Il y a une vingtaine d'années, les "hackers" n'existaient pas encore. Aujourd'hui, les dégâts qu'ils causent coûtent des milliards de dollars aux Etats-Unis.

CONCLUSION

Force est de constater que d'après les conférenciers, "Information Warfare" est une réalité. Une véritable collaboration va devoir se mettre en place pour pouvoir la combattre. Cette collaboration ne devra pas s'effectuer uniquement sur le plan national, mais aussi sur le plan international.

Nos dirigeants doivent être conscients des risques que comporte la société de l'information. La législation doit évoluer en ce sens, des normes internationales doivent être élaborées.

BIBLIOGRAPHIE SOMMAIRE

1. Information Warfare: Chaos on the Electronic Superhighway - Winn SCHWARTAU
C Thunder's Mouth Press, 1994, 432 pages.

2. Computer Crime: A Crimefighter's Handbook - David ICOVE, Karl SEGER et William VON STORCH, ^C O' Reilly and Associates, 1995, 437 pages.
3. Information Warfare: Protecting your Personal Security in the Computer Age - Winn SCHWARTAU, ^C Thunder's Mouth Press, 1996, 600 pages.
4. Netlaw: Your Rights in the Online World : Lance ROSE
Osborne Mc Graw-Hill, 1995, 372 pages.

Ces livres donnent au lecteur un bon aperçu des divers aspects de "l'Information Warfare". Le premier et le troisième livre sont d'ordre général, alors que le deuxième et le quatrième traitent respectivement de l'aspect criminel et juridique de la matière.

B. OPEN SOURCES SOLUTIONS

En 1995, un membre du Comité R avait participé au "Congrès OSS". A cette occasion, différentes recommandations ayant trait à l'utilisation des sources ouvertes (Voir rapport d'activités 1996, p. 198 à 210 incluses) ont été formulées.

Les sources ouvertes peuvent être définies comme étant toutes les sources d'information qui, légalement et éthiquement, sont accessibles au public, en contrepartie ou non d'un paiement.

Dans le cadre de leur mission de regroupement des informations, les services de police et de renseignement du monde entier sont de plus en plus convaincus de l'utilité de ces sources, négligées et oubliées par le passé.

Les avantages les plus souvent cités des sources ouvertes sont, entre autres, qu'elles sont particulièrement adéquates pour fournir des informations sur le contexte général d'une situation. Elles offrent aussi, lors de leur collecte, la possibilité de faire appel à des experts externes aux services (par exemple, à des bibliothécaires).

Ces sources devraient aussi pouvoir être réparties entre différents services, obligatoirement au niveau national et, accessoirement, au niveau international. Pour une discussion plus détaillée de ce concept, nous renvoyons, à nouveau, le lecteur au précédent rapport annuel.

Le congrès a été divisé en trois parties :

- les sources ouvertes et les informations économiques;
- les sources ouvertes et la sécurité nationale;
- les sources ouvertes et le maintien de l'ordre.

Lors de la première journée consacrée à la "Business Intelligence", on a surtout discuté d'Intranet. Intranet permet d'optimiser les connaissances et les informations présentes dans l'entreprise. Toutes les sources d'information sont ainsi rassemblées.

Pour permettre une bonne utilisation des informations, toutes les informations doivent être réunies dans une seule base de données. Il faudrait, à l'intérieur même de l'entreprise, développer un "browser" adapté aux besoins de l'entreprise.

L'accent a été mis sur le fait que l'information n'arrive pas toujours à la personne apte à en

comprendre le contenu.

Lors de ce congrès, on insista beaucoup sur le problème de la protection des informations. Pour de plus amples informations sur ce sujet, nous renvoyons le lecteur au commentaire à propos du congrès "InfoWarCon" mentionné ci-dessus.

Le volet "Law Enforcement" a été principalement consacré à la lutte contre le crime organisé et au rôle des sources ouvertes dans ce contexte. Comme l'avait relevé le congrès OSS1995, les sources d'informations pertinentes dans le cadre de la lutte contre la criminalité, sont légion.

La criminalité s'internationalise de plus en plus, avec pour conséquence que les informations portant uniquement sur l'environnement local d'un délit ou d'un crime ne suffisent plus.

On a insisté sur le fait qu' une détection précoce du crime international est déterminante pour le prévenir.

Ainsi, le porte-parole de la "Criminal Intelligence Division" australienne a remarqué que le développement des activités de la mafia japonaise en Australie s'inscrivait en grande partie dans le cadre d'une stratégie à long terme de cette organisation afin de s'emparer de la Côte Ouest américaine. Les orateurs ont donc plaidé en faveur d'une "Cultural Intelligence", une approche historique globale qui aboutit à une compréhension des causes du développement du crime organisé dans certaines régions du monde; ceci permettrait d'intervenir à temps.

De nombreux conférenciers ont abordé des sujets plus spécifiques, mais l'impression globale que laisse le Congrès-OSS est que "l'intelligence", sous toutes ses formes, est en pleine mutation.

Nous sommes dans l'ère de la société de l'information et de nombreux responsables des services de polices, de renseignement, de l'armée et du monde économique doivent s'adapter à cette croissance exponentielle des informations disponibles.

La valeur et l'utilité des congrès-OSS résident dans le fait que des personnes confrontées à des problèmes identiques se réunissent afin de discuter des solutions à trouver.

Dans ses conclusions finales, l'organisateur, Monsieur Steele, a promis de rendre la conférence de l'année prochaine plus pratique. C'est probablement une évolution positive, car les considérations théoriques de certains conférenciers ne sont pas toujours applicables dans la pratique.

Un rôle important de l'OSS est d'essayer de sensibiliser les décideurs politiques à ces problèmes.

CONCLUSION

Le Comité R souhaite que les décideurs politiques et les services de renseignement belges s'intéressent davantage à cette matière.

C. LAW ENFORCEMENT AND INTELLIGENCE

1. INTRODUCTION

Ce congrès a été organisé par "l'American Bar Association Standing Committee on Law and National Security".

Cette organisation fut fondée en 1962 par d'éminents juristes et universitaires; le but initial était de comparer l'Etat de droit américain avec la vision alternative que proposait le communisme international. Progressivement, ce mandat a été élargi à une fonction de conseil juridique sur de nombreux problèmes de sécurité nationale.

Depuis le début, "The Committee" a réalisé ses objectifs grâce à un programme de bourses d'études, de conférences et de publications. Un des grands mérites du "Committee" est d'être parvenu à augmenter de manière considérable, dans beaucoup de facultés de droit, le nombre de séminaires sur la législation relative à la sécurité nationale, passant notamment de 1 séminaire en 1974 à 83 séminaires en 1994. En 1990, on pouvait consulter des mémoires (casebooks) sur la législation en matière de sécurité nationale dans trois facultés de droit.

Les conférenciers et participants au débat étaient des personnalités de premier plan venues des Etats-Unis ou d'autres continents, et parmi elles d'anciens directeurs de la "Central Intelligence", "Deputy Attorneys General", "General Counsels" d'organismes clés comme la CIA et le FBI, ainsi que de nombreux universitaires et personnalités du monde des médias.

2. OBJET DU CONGRES

Le congrès a été consacré à la modification des relations entre "Law Enforcement" et "Intelligence" (renseignement).

Si le congrès a accordé une attention particulière à cette nouvelle problématique, il n'a pas manqué de mettre l'accent sur les risques que représentent encore à l'heure actuelle certains pays, (parmi ceux-ci, la Russie a été citée).

La Russie est un pays aujourd'hui complètement désorganisé qui dispose d'une grande quantité d'armes nucléaires, objets d'une contrebande à grande échelle. Le crime organisé y est implanté à tous les niveaux de la société. La principale crainte est de voir ces armes nucléaires utilisées par des terroristes.

A l'avenir, l'espionnage redeviendra également un sujet important, parce qu'il a de plus en plus pour cible des industries.

Enfin, sans parler de l' "Information Warfare", de nombreuses menaces se concentrent sur certains secteurs vitaux tels que les banques, la distribution de l'eau, les réseaux informatiques, etc...

Dorénavant, la société n'est plus uniquement agressée avec des armes traditionnelles. L'évolution du monde informatisé crée de nouvelles armes qui peuvent mettre en danger la sécurité nationale.

3. DIFFERENCES HABITUELLES ENTRE "INTELLIGENCE" ET "LAW ENFORCEMENT"

Jadis, "Law Enforcement" et "Intelligence" poursuivaient des objectifs différents, n'avaient pas les mêmes règles, et utilisaient d'autres sources et méthodes.

Les services de renseignement rassemblaient des informations pour aider les dirigeants, principalement dans le domaine de la sécurité nationale. Les services de police collectaient des informations dans le but d'entamer des poursuites judiciaires.

A cet égard, Michael A. Vatis, Associate Deputy Attorney General (U.S. Department of Justice), définit le "Law Enforcement" comme "*Investigation, apprehension and prosecution*".

Aux Etats-Unis, on part du principe que les services de renseignement n'ont pas de compétences policières et qu'ils n'enquêtent pas au sujet des activités de citoyens américains.

Il existe peu de règles applicables à la collecte d'informations effectuée par les services de renseignement. En effet, les services de renseignement rassemblent surtout des informations en vue de la sécurité nationale d'une part et d'autre part, cette collecte d'informations concerne habituellement des activités à l'étranger et non des activités de citoyens américains.

Par contre, le "Bill of Rights" ainsi que d'autres normes et décisions judiciaires règlent les enquêtes de police.

Sur le plan des attentes en terme de qualité des informations réunies, une grande différence existe entre la collecte de l'information réalisée par un service de renseignement et celle effectuée par un service de police.

Tout d'abord, les informations réunies par les services de renseignement sont généralement des informations "brutes" d'une crédibilité sujette à caution mais qui, après un travail d'analyse soigneux, peuvent être transformées en renseignement, qui, bien qu'encore parfois partiellement inexact, peut tout de même être utile aux décideurs politiques.

Les informations rassemblées par les services de police doivent être suffisamment fiables pour être utilisées comme pièces à conviction dans un procès.

Ensuite, les sources et méthodes sont différentes d'un service à l'autre.

Les services de police récoltent leurs informations par des auditions, des informateurs occasionnels, ou encore une surveillance physique et électronique.

L'"Intelligence Information" provient souvent d'une reconnaissance photographique, de l'interception de signaux radio et de l'utilisation d'informateurs à long terme recrutés à l'étranger par des agents des services de renseignement.

Enfin, les deux types de services font appel à leurs relations avec les services étrangers et utilisent les sources ouvertes.

4. SITUATION PENDANT ET APRES LA GUERRE FROIDE

4.1. Pendant la guerre froide

Durant la guerre froide, il existait un réel cloisonnement entre les services qui s'occupaient de la lutte contre la criminalité (dont le plus important est le FBI) et les services qui se chargeaient de la sécurité nationale (tels que la NSA et la CIA).

Le "National Security Act" [*Loi sur la Sécurité Nationale*] de 1947 est très clair à propos de cette problématique : la CIA n'a pas de compétences policières et ne peut procéder à aucune arrestation ni perquisition.

Les efforts des services de renseignement se concentraient entièrement sur l'étranger (l'ex-URSS, ses états satellites et les régimes communistes, essentiellement en Amérique Latine), alors que les services de police s'occupaient des affaires intérieures.

Le FBI avait une mission limitée à l'étranger, exercée par des officiers de liaison en poste dans les ambassades américaines. Cependant, la criminalité était essentiellement considérée comme un problème intérieur.

A l'époque, le terrorisme et la criminalité organisée étaient, dans une certaine mesure, déjà présents au niveau international, mais les services de renseignement ne disposaient pas d'effectifs suffisants pour combattre ces phénomènes.

4.2. Après la guerre froide

Le cloisonnement géographique et fonctionnel entre les services de renseignement et les services de police, qui empêchait tout chevauchement entre leurs missions, a pris fin lors des dix dernières années en raison de la survenance de deux événements.

De nouveaux problèmes concernant le terrorisme et l'attention récente portée à la lutte antidrogue ont conduit les services de police à s'investir de façon plus active à l'étranger. Aujourd'hui, les statuts du FBI lui permettent de mener des enquêtes sur des attentats terroristes visant des citoyens et des avions américains, où qu'ils soient commis.

Ces statuts permettent au "Prosecutor" (procureur) fédéral de faire juger ces affaires aux Etats-Unis lorsque l'extradition des terroristes impliqués peut être obtenue.

Durant cette même période, un second événement important s'est produit : le démembrement de l'ex-Union Soviétique.

La menace représentée par l'Union soviétique disparue, l'attention des services de renseignement s'est reportée sur d'autres problèmes tels que la drogue, le terrorisme, la prolifération des armes, bref sur des domaines que traitent aussi les services de police.

L'importance que les services de renseignement allaient attacher à ces matières fut aussi dictée par des raisons budgétaires. En effet, compte tenu de la disparition de leur mission principale, il fut question que le "National Congress" réduise leur budget. Ces services ne pouvaient donc justifier le maintien de leurs budgets que par de nouvelles missions.

5. SITUATION ACTUELLE

Légiférer en matière de sécurité nationale représente une tâche difficile et pourtant d'un intérêt primordial, en vue de sauvegarder la Constitution et la Nation.

Il existe ainsi aujourd'hui différents domaines dans lesquels les activités de deux services se recouvrent, ils partagent des responsabilités.

Après la fin de la guerre froide, de nouveaux problèmes sont apparus, comme la possibilité pour les terroristes de s'approprier des armes nucléaires et biologiques. La situation géo-politique est devenue plus complexe de manière telle que les réseaux de renseignement se sont davantage impliqués dans la lutte contre la criminalité internationale.

A l'heure actuelle, la CIA et le FBI, pour la première fois dans leur histoire, réfléchissent ensemble sur le terrorisme (réunions de personnel opérationnel). Les deux services sont représentés au "Counterterrorist Center", un service d'analyse chargé de rassembler des informations sur des groupes terroristes, leurs opérations, leurs installations d'entraînement, leurs méthodes de recrutement, etc...

Il est clair qu'aujourd'hui, le cloisonnement strict entre "Law Enforcement" et "Intelligence" n'est plus possible ni souhaitable.

6. MESURES POUR ANTICIPER L'ÉVOLUTION DE LA NOUVELLE SITUATION

Deux éléments apparaissent d'une importance capitale :

- Tout d'abord, il importe d'établir des directives pour permettre et mener à bien les enquêtes communes de la CIA et du FBI. A cette fin, un groupe de travail a été constitué au sein du ministère de la Justice.

Ce volet ne posera pas beaucoup de problèmes, du moins pas d'un point de vue légal, il est possible de fixer des règles et des critères clairs, pour déterminer dans quels cas des enquêtes communes peuvent être menées.

On envisage une formation commune pour familiariser chaque service aux méthodes de l'autre. Enfin, toutes les informations devront être rassemblées avec pour objectif de servir de preuves lors des poursuites devant un tribunal. Ceci évitera de devoir dévoiler au tribunal des informations susceptibles de compromettre la sécurité nationale pour obtenir une condamnation judiciaire.

- L'aspect "renseignement" pose, quant à lui, plus de problèmes : à savoir l'utilisation dans des enquêtes policières d'informations recueillies à des fins de renseignement .

Certains experts doutent que de telles informations soient a priori utilisables à des fins policières. En effet, le manque de fiabilité du "renseignement" a déjà été souligné; il repose parfois sur de simples supputations faites à partir de faits connus. Ce type d'information correspond à ce que les décideurs politiques attendent des services de renseignement, à savoir, les prévisions sur des événements.

Utiliser ces informations dans un tribunal pour, par exemple, obtenir la condamnation d'un terroriste est une tout autre affaire. Il est dès lors préférable de chercher une solution de compromis dans une collaboration partielle entre services de police et de renseignement.

7. LEGISLATION - PROBLEMATIQUE

7.1. "La règle de Brady"

L'application de la règle dite "de Brady" pose un problème majeur.

En effet, la Cour suprême des Etats-Unis a décidé en 1963 qu'au cours d'un procès, le "prosecutor"

⁽¹⁾ devait aussi rechercher, parmi toutes les informations qui sont à sa disposition, des indices favorables à la défense.

Cette règle obligerait donc, le cas échéant, le "prosecutor" à parcourir les dossiers des services de renseignement dans le but de trouver des indices à décharges. Ceci pourrait provoquer un conflit entre le "prosecutor" et les services de renseignement qui, en aucun cas, n'accepteront que la défense prenne connaissance d'informations touchant à la sécurité nationale. Ces services pourraient même chercher à ce que le "prosecutor" classe l'affaire sans suite.

7.2. Solutions possibles

Un système judiciaire consisterait à centraliser au ministère de la Justice toutes les requêtes des services de police visant à obtenir des informations auprès des services de renseignement dans le cadre d'une enquête. Un service juridique se chargerait alors d'évaluer la possibilité de faire droit à chaque requête.

Les informations du service de renseignement seront uniquement utilisées comme un "Investigative lead", c'est-à-dire comme base d'investigation, et non comme une preuve irréfutable devant un tribunal.

Cette proposition de nouvelle procédure est de nature à répondre aux exigences de "l'arrêt Brady".

Si cette procédure s'avérait impossible à mettre en oeuvre, le "Classified Information Procedures Act" peut être invoquée.

Cette loi stipule que les informations secrètes ne doivent pas être divulguées si elles ne sont pas essentielles à la défense, ou si le gouvernement expurge le document, en manière telle que l'information substantielle puisse tout de même être fournie à la défense sans pour autant mettre en danger les "méthodes et sources" des services de renseignement.

7.3. Constatation

L'ébauche d'un système sans faille constitue un véritable défi et provoquera de nombreuses discussions.

Cependant, il convient de remarquer que, jusqu'à présent, aucun abus de pouvoir dans le chef des services de renseignement n'a été constaté sur le plan des compétences du "Law Enforcement".

De plus, il s'agit ici de problèmes très sérieux qui, s'ils ne sont pas abordés de façon professionnelle, peuvent coûter beaucoup de vies humaines.

C'est pourquoi l'économie d'un débat ne peut être faite en invoquant uniquement un risque éventuel de violations des droits et des libertés consacrés par la Constitution.

8. COLLABORATION INTERNATIONALE

La problématique de la collaboration entre "Law Enforcement" et "Intelligence" en Grande-Bretagne

⁽¹⁾ Partie poursuivante, sorte d'équivalent du ministère public en Belgique

a aussi été abordée au cours de ce congrès. En fin de compte, il ne s'agit pas d'envisager uniquement la façon dont se déroule la collaboration entre ces services, mais la question dans un contexte international.

Le monde n'est plus régi par le dogme politique mais par les nécessités économiques. Les menaces sont internationales et n'émanent plus d'un seul bloc. La sphère d'influence, le pouvoir économique et les moyens d'action complexes des syndicats du crime sont plus puissants que la plupart des Etats qui composent les Nations Unies.

Le terrorisme et le crime organisé ne sont pas des phénomènes nouveaux, mais les nouvelles technologies permettent au crime organisé de créer des réseaux mondiaux.

La réponse se doit donc d'être adaptée.

Pour ce faire, il est essentiel de faire appel à la coopération internationale qui tente de remédier aux différences des multiples procédures.

Une nouvelle approche juridique internationale doit être définie pour affronter les menaces internationales. Cela implique la collecte d'informations pertinentes et correctes.

Pour ces raisons, es organisations qui recueillent des informations électroniques tels que la NSA et le GCHQ doivent être impliquées dans le combat contre les menaces criminelles.

Si nécessaire, les services de renseignement doivent s'intégrer dans le processus légal et transmettre des informations pour les besoins du "Law Enforcement". Le MI 5 et la police doivent collaborer contre le crime organisé. "Intelligence" et "Law Inforcement" doivent surtout unir leurs forces pour combattre le terrorisme.

Le problème qui se pose à ce stade est la transformation des informations des services de renseignement en preuves. Les services de renseignement doivent continuer à protéger les documents classifiés qui ne sont pas significatifs dans le cadre de la procédure. Le défi à relever consiste à décider quelles sont les pièces probantes et de savoir dans quelle mesure elles peuvent être utilisées.

Les compétences des services de renseignement et de police sont les éléments fondamentaux de la protection de la sécurité nationale pour en répondre aux nouvelles menaces.

La coopération entre "Law Enforcement" et "L'intelligence" doit aboutir à l'élaboration d'une législation internationale qui harmonise les lois et procédures nationales.

9. CONCLUSIONS

- Aux Etats-Unis et en Grande-Bretagne, tout comme chez nous, on a adopté une position qui n'attribue pas aux services de renseignement des compétences policières.
- Depuis la fin de la guerre froide, de nouveaux problèmes, tels que la possibilité pour les terroristes d'acquérir des armes nucléaires et biologiques, et la complexification croissante de la situation géopolitique, ont conduit les services de renseignement à jouer un rôle dans la lutte contre la criminalité internationale.
Pour la combattre de façon efficace, une collaboration étroite entre les services de renseignement et les services de police s'impose.

- Les problèmes juridiques liés à cette collaboration ne doivent pas être sous-estimés.
- La collaboration entre ces services demande donc une gestion, une formation, une coordination et surtout une communication qui soient à l'optimum.
- L'élaboration de directives définissant cette collaboration entre les deux types de services, à l'exemple des Etats-Unis, est indispensable à la réalisation de ces objectifs.
- Il faut encourager l'organisation de formations communes aux deux services, qui permettent aux uns et aux autres de se familiariser à leurs méthodes respectives.
- Enfin, la lutte contre les formes violentes de la criminalité internationale ne pourra se dérouler efficacement que dans le cadre d'une coopération internationale et à condition de définir une nouvelle approche juridique internationale. L'adoption de normes internationales s'impose.

CHAPITRE 2 : EUROPE HORIZON 2000 : NOUVELLES MENACES, NOUVEAUX TERRORISMES

Un membre du Comité R et un membre du Service d'enquêtes ont participé, à Bruxelles le 28 novembre 1996, à la journée d'étude, organisée par le "Groupe International de Recherche et d'Information sur la Sécurité" (G.I.R.I.S.) et "l'Institut de Criminologie de Paris". Le thème de cette journée d'étude s'intitulait "Nouvelles menaces , nouveaux terrorismes".

L'Europe, ces derniers temps, est confrontée à de nouvelles menaces et de nouveaux terrorismes.

Sir Colin McColl, diplomate, ancien chef du MI6, a exposé qu'un nouveau capitalisme non contrôlé est né dans lequel (fin de la guerre froide, l'omniprésence des médias, les nouvelles technologies) le monde politique a, pour plusieurs raisons, subi un choc qui l'a immobilisé. Dans ce nouveau monde, les riches de l'Ouest deviennent de plus en plus riches tandis que les pauvres se sentent de plus en plus dépouillés. Ce déséquilibre, accompagné d'un manque de réaction du monde politique, offre un terrain fertile pour ses activités déstabilisant les démocraties, au terrorisme dans le domaine de la haute technologie et au crime organisé,. La mission principale de l'Europe n'est pas de promouvoir la démocratie mais bien de rétablir un équilibre économique.

Xavier Raufer, chargé de cours à l'Institut de Criminologie à Paris, a défini les nouvelles menaces politiques de niveau stratégique. Après la chute du mur de Berlin, d'autres formes, non gouvernementales et transnationales telles que la mafia et les milices ont pris la place des anciens groupements terroristes bien organisés (ETA basque, OLP palestinienne). Le terrorisme de la guerre froide a été remplacé par une menace où des extrémistes fondamentalistes, malgré les répressions dont ils font l'objet, font vaciller les régimes (Groupe Islamique Armé) et où des organisations criminelles internationales (cartels de drogue, triades) et des mouvements de guérillas dégénérés (les tigres Tamoul) jouent un rôle primordial. Il est essentiel que cette menace soit considérée comme prioritaire et combattue avec des moyens très sophistiqués (systèmes informatiques, satellites d'observation, réseaux de télécommunication) aussi bien par les services de police et de sécurité que par les militaires

Irène Stoller, chef de la section antiterroriste du parquet de Paris, a décrit la législation française et les méthodes policières qui permettent, en France, de lutter contre le fléau du terrorisme représenté principalement par le "FLNC" et le terrorisme religieux qu'elle appelle les "gangsterroristes". Elle dénomme aussi ce type de terrorisme "hybride politico-criminel". Ce haut magistrat a mis l'accent sur la centralisation des services de police qui constitue un appui indispensable à l'action poursuivie par la magistrature française.

François Haut, de l'Institut de Criminologie à Paris, a traité de la problématique politico-criminelle de type hybride menée par les mouvements de guérilla qui ont dégénéré. Deux exemples ont été cités : "Les tigres tamouls" et le PKK qui ne s'occupent pas uniquement de leur lutte politique mais entretiennent des relations avec des organisations criminelles et collaborent avec eux à l'occasion

de trafics d'armes et de drogues.

Bruce Hoffman, directeur du "Centre for the Study of Terrorism and Political violence" de l'Université de Saint-Andrews (Royaume-Uni), a fait part de l'étude qu'il a menée à propos du terrorisme basé sur un fanatisme religieux.

Jean-Pierre Doraene, a évoqué la dimension financière des nouvelles menaces. Il est le chef de l'Office Central de lutte contre la délinquance économique et financière organisée (OCDEFO), un organisme officiel qui s'occupe en Belgique de la lutte contre le blanchiment de capitaux. Après avoir décrit les différentes pratiques, il a expliqué les différents aspects de cette menace telles que la fraude fiscale, l'utilisation de comptes en banques et la création de sociétés écran. Une coopération policière internationale constitue, selon l'orateur, le meilleur moyen de lutter contre cette forme de criminalité.

Le Professeur Karl-Heinz Kamp, du "Konrad Adenauer Stiftung" a parlé des risques liés aux trafics nucléaires. Il estime utopique l'éventualité suivant laquelle l'une ou l'autre organisation non-gouvernementale fabrique une bombe nucléaire. Cette utopie, entretenue par certains médias, ne constitue pas vraiment une menace. Par contre le risque d'attentat commis par un déséquilibré, ou par une secte suicidaire, faisant usage de matières fissiles volées ou rachetées illégalement dans le but de contaminer une grande partie de la population, est beaucoup plus important. Il est indispensable de rester vigilant.

Le Professeur Ariel Merari de l'université de Tel Aviv a clôturé la journée d'étude. Il constate que le terrorisme n'a pas changé ni dans sa présentation ni dans ses méthodes, si on le compare à la guerre conventionnelle qui, elle, a évolué avec les nouvelles technologies. Le terrorisme poursuit son combat comme il y a 50 ou 100 ans. Seul le détournement d'avion peut être considéré comme une nouvelle tactique. Les raisons doivent en être trouvées dans la logistique indispensable à ce type d'action. Un manque de qualification technique des militants terroristes explique que la plupart des groupes terroristes à vocation politique répugnent à faire usage de moyens trop sophistiqués qui pourraient se retourner contre eux en cas d'utilisation inadéquate. Ces méthodes sont souvent contre-productives car elles font perdre le crédit de la population que ces groupes entendent supporter. Enfin, sur le plan psychologique, des attentats barbares peuvent avoir une influence néfaste sur la motivation de leurs militants.

En guise de conclusion, on peut affirmer que le terrorisme continuera d'exister. Dans ce jeu du chat et de la souris que mènent les terroristes et les autorités, ces dernières sont constamment une guerre en retard. Il faut veiller à ne pas commettre l'erreur d'augmenter la pression policière en prenant des mesures tellement coercitives qu'elles empêchent une vie normale de la population. Par contre, il faut combattre le terrorisme en cherchant ses failles et en les exploitant.

Commentaires

En général, les orateurs de la journée d'études ne se sont pas montrés optimistes. Plusieurs d'entre eux ont insisté sur la nécessité absolue d'une collaboration internationale et sur l'usage de moyens de communication et d'observation modernes et sophistiqués. Les services de renseignement doivent aussi collaborer au combat contre le terrorisme.

La problématique du "crime organisé" n'a été abordé qu'indirectement à l'occasion des exposés donnés sur des organisations politico-criminelles et sur le blanchissement de l'argent. A ce propos, on attirera l'attention sur les trafics de drogue, d'armes et les sociétés-écran.

CHAPITRE 3 : SÉMINAIRE “INTERNET FACE AU DROIT”

La lecture d'ouvrages spécialisés nous apprend que l'essor du réseau Internet intéresse les services de renseignement du monde entier (voir notamment "*Guerre dans le cyberspace*" - Jean Guisnel - Edition La découverte, octobre 1995). Cette problématique retient l'attention du Comité R. C'est pourquoi trois membres du Comité R ont assisté à ce séminaire "*Internet face au Droit*" organisé par le Centre de recherche droit et informatique (CRID) des Facultés universitaires Notre Dame de la Paix (FUNDP) à Namur les 21 et 22 novembre 1996. Quelques exposés ont particulièrement retenu l'attention du Comité R.

Monsieur Etienne Montero, chargé de cours aux FUNDP, a traité des responsabilités liées à la diffusion d'informations illicites ou inexactes sur Internet. Pour les uns, Internet est un nouvel espace de liberté totale et sans bornes; ils ont tendance à crier à la censure si d'aucuns s'avisent de rappeler que des règles existent et qu'Internet n'y échappe pas. D'autres, au contraire, en appellent à des mesures de contrôle, voire à la censure préalable, et réclament l'adoption de réglementations spécifiques et contraignantes. Des deux côtés, l'erreur procède d'une même méconnaissance de ce qu'est au juste Internet, considéré comme un "espace virtuel", étranger au "monde réel". Le droit actuel serait donc inapte à régir les actes délictueux commis dans le soi-disant nouveau "monde virtuel". Le professeur Montero s'est attaché à montrer la fausseté de pareille perception, sans vouloir en nier pour autant certaines difficultés inhérentes à la mise en oeuvre des responsabilités. En réalité, les obstacles tiennent, pour la plupart, à la complexité du droit tout simplement.

Philippe Gérard et Valérie Willems se sont penchés sur la prévention et la répression de la criminalité sur Internet. Pour eux, la multiplicité des acteurs et la question de leur responsabilité respective constituent les principales difficultés.

Monsieur Etienne Davio a traité le problème de la signature électronique et de la cryptographie des messages échangés sur Internet. Cette problématique est celle dont s'occupe le groupe Belinfosec et il en est d'ailleurs question au titre II - B - chapitre 4 du présent rapport. La cryptographie peut être utilisée, non seulement comme moyen de sécurité, mais aussi comme moyen de signature électronique, c'est-à-dire comme moyen d'identification de l'interlocuteur. Le rôle et la responsabilité des futures autorités de certification des clés cryptographiques devront être précisés.

Mesdames Marie-Hélène Boulanger et Cécile de Terwagne ont développé le thème du respect de la vie privée sur Internet. Elles ont expliqué qu'il est possible de récolter des données personnelles sur les utilisateurs d'Internet. En identifiant les postes (et les personnes) qui consultent certains sites commerciaux, de même qu'en établissant la fréquence et la durée de ces consultations, il est par exemple possible de dessiner le profil des consommateurs potentiels.

Madame Anne Troye-Walker a exposé les problèmes relatifs à la conclusion de contrats par Internet. Elle a présenté les principales lois et conventions internationales applicables en la matière. En juin 1996, un modèle de loi sur le Commerce électronique international a été proposé à tous les pays membres des Nations Unies.

D'autres thèmes furent aussi abordés dont l'intérêt était moindre pour le Comité R : Internet et la propriété intellectuelle, Internet et les modes de régulation.

CHAPITRE 4: RENCONTRE DU COMITÉ R AVEC LA DÉLÉGATION UKRAINIENNE

Le conseiller du ministre de la Défense nationale a demandé au Comité R de recevoir le secrétaire du Conseil de Sécurité nationale et de Défense de l'Ukraine, Monsieur Volodymir Horbulin, accompagné de l'ambassadeur de l'Ukraine en Belgique, Monsieur Borys Tarasyuk et des attachés militaires de l'ambassade ukrainienne.

Cette rencontre eut lieu le 9 janvier 1997 au siège du Comité R.

La présidente, après avoir remercié les invités de leur présence qui s'inscrit dans le cadre des bonnes relations entre l'Ukraine et la Belgique, a exposé les différentes législations étrangères, qui règlent les activités et le contrôle des services de renseignement et qui furent étudiées par le Comité R ces deux dernières années.

Les rapports d'activités du Comité R ainsi que le projet de loi organique des services de renseignement et de sécurité actuellement en discussion au Parlement ont été remis à la délégation ukrainienne afin de leur permettre de suivre l'exposé.

- La problématique des activités des services de renseignement en décrivant le cycle du renseignement a été rappelée.
- Une description du contenu de la loi sur les services de renseignement a été donnée, à partir de l'étude des législations allemande, portugaise, canadienne, néerlandaise, britannique, italienne et américaine (rapport d'activités 1995 - p.4 à 35 et rapport d'activités 1996 - p. 2 à 18).
- Les différents types de services de renseignement furent énumérés.
- La définition des missions dans une loi :
Les articles 7 et 9 du projet de loi belge discuté actuellement au Parlement ont été examinés. La question de savoir s'il faut donner au service de police une compétence de renseignement (comme pour le FBI et le Service de renseignement civil Ukrainien (SBU) fut évoquée.
- Une discussion sur la problématique de la criminalité organisée s'est engagée.
- L'organisation des services et la responsabilité du ministre de tutelle devant le Parlement.
- Les méthodes et l'exercice des missions.

- La collaboration des services de renseignement, mais aussi celle avec les services de police et avec toute autre administration est un des aspects qui fut souligné car, il est indissociable de l'efficacité de ces services.
- La coordination.
Une bonne coordination des activités des services est indispensable pour éviter la guerre des services ou pour empêcher les ministres de tutelle d' utiliser ces services à leur fin personnelle et non plus dans l'intérêt de l'Etat.
- Le contrôle démocratique.
La loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et son application par le Comité R ont été longuement examinées. C'est ce point qui a particulièrement intéressé la délégation ukrainienne.

CHAPITRE 5 : COLLOQUE SUR L'INTELLIGENCE ÉCONOMIQUE À PARIS

Le projet de loi sur les services de renseignement du 20 juin 1996 attribue à la Sûreté de l'Etat une nouvelle mission en son article 7 § 1^{er}, 1^o ; § 2, 3^o et § 3. En effet cet article stipule :

“La Sûreté de l'Etat a pour missions :

§ 1^{er}, 1^o *de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure de l'Etat et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'Etat et les relations internationales, ou le potentiel scientifique ou économique du pays et d'en informer sans délai les ministres compétents.*

§ 2, 3^o *“le potentiel scientifique ou économique du pays” : la sauvegarde des éléments essentiels du potentiel scientifique ou économique déterminés par le Comité ministériel contre toute menace d'atteinte grave par des moyens illicites, trompeurs ou clandestins.*

§ 3. *A la requête de la Sûreté de l'Etat, le Service général du renseignement et de la sécurité prête son concours à celle-ci pour recueillir le renseignement lorsque des militaires sont impliqués dans des activités visées au § 1^{er}, 1^o.*

Le Comité R a estimé qu'il convenait, pour effectuer sa mission de contrôle, de s'intéresser à cette problématique. Tous les services de renseignements étrangers des pays industrialisés remplissent cette mission depuis des années. C'est pour cette raison qu'un des membres du Comité R a assisté à ce colloque.

L'intelligence économique et concurrentielle est définie par D. Rouach, professeur à l'Ecole des Affaires de la manière suivante :

“ C'est l'ensemble des actions de recherche, de traitement, de diffusion et de protection de l'information utile aux différents acteurs économiques”.

Il a été beaucoup question lors de ce colloque d'un autre concept : la veille stratégique et technologique. Henri Dou dans son ouvrage *“La veille technologique”* en donne la définition suivante :

“ La veille stratégique c'est l'observation et l'analyse de l'environnement suivies de la diffusion, bien ciblée des informations sélectionnées et traitées, utiles à la prise de décision stratégique.”

Ces notions recouvrent l'ensemble des activités du renseignement économique. C'est ce dernier point qui les différencie des services de renseignement.

Ce n'est que depuis le début des années 1980-1985 qu'est apparue une politique de renseignement économique. Dans les années 1990, le secteur s'est professionnalisé.

La plupart des exposés furent consacrés à l'intelligence économique au sein de l'entreprise. L'intervention ou la collaboration de l'Etat avec les entreprises fut aussi abordée.

La République Française, par l'intermédiaire du Commissariat au plan, a, depuis février 1994, donné ses lettres de noblesse à l'intelligence économique en publiant un rapport décrivant en détail tous les acteurs publics et para-publics de ce secteur.

Son auteur, Jean-Louis Levet, préconise en recommandations que le Secrétariat général de la défense nationale (SGDN), qui dépend du Premier ministre, soit l'instance de coordination des initiatives et de l'action de l'Etat dans le monde du renseignement⁽¹⁾.

Une autre recommandation prône la création d'un réseau de hauts fonctionnaires en intelligence économique. La troisième recommandation vise à élaborer un plan de sensibilisation et de formation des acteurs publics et para-publics.

La première de ces propositions a été avalisée par le gouvernement français suivant les participants au colloque. En effet, le SGDN coordonne les activités des services de renseignement. Toujours selon les personnes rencontrées, cette coordination balbutie à l'heure actuelle.

Il est utile de rappeler ici que la France a institué six services de renseignement :

1. La Direction Générale de la Sécurité Extérieure (DGSE) : service militaire de renseignement extérieur.
2. La Direction de la Protection et de la Sécurité de la Défense (DPSD) : service de renseignement militaire intérieur chargé principalement du contre-espionnage et des habilitations de sécurité.
3. La Direction du Renseignement Militaire (DRM), chargée notamment de l'analyse et du traitement des photos satellites.
4. La Direction de la Surveillance du Territoire (DST), service civil chargé notamment du contre-espionnage et du terrorisme. Cette direction se trouve sous la tutelle du ministre de l'Intérieur, à l'inverse des trois premiers services énumérés ci-dessus qui sont placés sous la responsabilité du ministre de la Défense nationale.
5. La Direction Centrale des Renseignements Généraux (DCRG) qui exerce le métier de renseignement politique (élections ...), le plus secret des services français se trouvant sous la responsabilité du ministre de l'Intérieur.
6. Le Secrétariat Général de la Défense Nationale (SGDN) qui dépend comme indiqué ci-dessus du Premier ministre et qui est notamment chargé de la coordination des activités des différents services de renseignement.

Edouard Valensi, Directeur du Centre de Documentation de l'Armement (CEDOCAR-Ministère de la Défense nationale), a exposé l'importance qu'il y a à différencier une information à valeur ajoutée d'une fausse information.

Le CEDOCAR section vivant indépendamment de la Délégation Générale pour l'Armement (DGA), dépendant elle-même du ministère de la Défense Nationale, fournit aux forces armées françaises

⁽¹⁾ Le Monde du Renseignement n° 284, 21 mars 1996

et à la communauté du renseignement, publique ou privée, l'information documentaire dont elles ont besoin. C'est à ce titre que son directeur a participé au séminaire.

Cette administration, gérant un budget annuel d'environ 70 millions de francs français et se composant d'environ 200 fonctionnaires, possède une banque de données exceptionnellement riche : 2000 CD Rom en réseau, des brevets européens et américains, une revue de presse mondiale et toute publication concernant notamment l'électronique ou l'aéronautique.

En professionnel de l'information, son directeur n'a pas manqué de donner un numéro de téléphone auquel des informations pouvaient être recueillies : 00-33-1-45-52-45-01 (Melle. Maréchal).

Quelques recettes ont été données par Monsieur E. Valensi :

- Plus une information est fautive, mieux elle est accueillie.
- La presse parle souvent et abondamment des études relatives à de nouveaux produits. La plupart du temps, la mise en oeuvre du projet né de l'étude devient secrète. En conséquence, si l'on veut rechercher le contenu d'un secret, il faut se référer aux écrits parus au moment de l'élaboration des études du projet.
Il n'y a pas de projets importants sans engagement d'un budget à leur mesure.

D'autres orateurs ont abordé la manière de recueillir le renseignement, dénommé dans le monde économique "Intelligence économique et concurrentielle". Les méthodes utilisées à cet égard ne divergent guère de celles employées par les services de renseignement des états.

Certains ont souligné que le Japon fut un précurseur dans ce domaine. Beaucoup ont insisté sur les méthodes agressives des Etats-Unis ou de l'Allemagne dans la guerre économique.

Les Français considèrent qu'il est important que les patrons des entreprises soient sensibilisés à l'importance de la création au sein de leur entreprise d'une cellule structurée d'intelligence économique concurrentielle.

Lors des interruptions de séances, presque tous les participants venant de firmes telles que Elf Aquitaine, Thompson - CSF, EDF, Matra, Cap systèmes, Rhône Poulenc, Rorer SA, Hutchinson, Dassault, Nestlé France ou encore, sans pouvoir toutes les citer, Mc Kinsey & Company, ont dit leurs difficultés à convaincre leur patron de la nécessité de structurer une section d'intelligence économique et concurrentielle.

Lors d'une discussion avec des participants au cours d'un déjeuner, il est apparu qu'une collaboration informelle existe entre les agents des services de renseignement et le personnel de ces firmes. Un réel échange d'information s'effectue, basé sur des relations humaines et s'exécutant sur le mode du donnant-donnant. Ainsi le secteur privé cultive ses relations avec le CEDOCAR, qui lui rend des services, ou avec la Direction des Relations Internationales, une des sections de la DGA, ou encore avec les services de renseignement eux-mêmes.

Les cadres de société, après une visite d'une usine dans un pays étranger, établissent un mémo qu'ils transmettent aux services de renseignement. Lorsque ces cadres ont besoin d'une information, ils s'adressent à leur "honorabile correspondant" qui leur répond : *"On va voir ce que l'on peut faire"*.

Il s'agit d'un réseau cloisonné. Les relations s'établissent de personne à personne. Lorsqu'une des deux parties quitte le secteur, il présente son remplaçant à son "honorabile correspondant". Le réseau perdure.

La motivation principale des cadres à participer à ce séminaire est le besoin de savoir ce qu'il faut faire pour d'une part, convaincre le patron de la nécessité de créer au sein de l'entreprise une cellule d'intelligence économique et concurrentielle, et d'autre part, ce qu'il faut faire pour professionnaliser le secteur de la veille économique.

A la première question, il a été répondu que l'essentiel était de démontrer que l'intelligence économique pouvait à court terme rapporter beaucoup d'argent.

A la seconde question, des modèles de structure impliquant une bonne collaboration avec tous les acteurs du monde du renseignement ont été apportés.

Enfin l'importance de la protection du patrimoine économique français a été mis en exergue par plusieurs orateurs.

CONCLUSIONS

La Belgique ne possède pas ou peu de ressources naturelles. Ses richesses sont principalement d'ordre intellectuel. Il est essentiel que ce patrimoine soit protégé.

Le gouvernement l'a compris puisque le projet de loi organique des services de renseignement charge la Sûreté de l'Etat d'une mission de renseignement économique.

Un comité pour la compétitivité et la sécurité économique a été créé en France par décret du 1^{er} avril 1995. Ce comité constitue un nouveau dispositif national d'intelligence économique. Il a vu le jour à l'initiative du Secrétariat Général de la Défense Nationale et a été agréé par le gouvernement.

Placé sous la présidence du Premier ministre, aujourd'hui, par délégation, sous la responsabilité du ministre de l'Economie, des Finances et du Plan, ce comité a pour mission "d'éclairer de ses avis le Premier ministre sur les questions de compétitivité et de sécurité économique".

Les personnalités qui le composent, représentent l'industrie, la finance et le monde scientifique. Ils auront pour mission de fixer les grandes orientations stratégiques et prospectives en matière de compétitivité et de sécurité économique ⁽²⁾.

Le SGDN en assure le secrétariat au titre de ses attributions en matière de défense et de sécurité économique.

Ce comité a relevé l'importance qui est accordée à cette problématique dans certains pays industrialisés dans la mesure où la responsabilité de ce type de comité est attribuée au Premier ministre en France. Aux Etats-Unis, cette question a été prise en charge par le Président lui-même.

Il apparaît des exposés faits lors du congrès OSS '96 à Washington ⁽³⁾ que les spécialistes de cette matière dans le monde estiment que cette institution constitue une excellente innovation.

En ce qui concerne la Belgique, le Comité R estime que les relations sporadiques qui existent entre les services de renseignements belges et les entreprises doivent se développer. Ces relations permettront d'assurer l'assiette du recueil des informations indispensable au contrôle de la guerre économique.

La coordination des services de renseignement s'effectuera grâce à la plate forme que constitue le collège du renseignement.

⁽²⁾ Défense n° 70 - décembre 1995 - Philippe Clerc - La compétitivité et la sécurité économique: un enjeu stratégique pour la France.

Le ministère des Affaires économiques pourrait comporter une section analogue à celle mise en place en France sous la dénomination 'Comité pour la compétitivité et la sécurité économique'. Les entreprises belges pourraient s'adresser à cette section du ministère des Affaires économiques pour obtenir le renseignement indispensable à une meilleure rentabilité des firmes belges. Cette section recevrait les demandes émanant des entreprises et les transmettrait à la Sûreté de l'Etat. Elle devrait nécessairement être en relation constante avec le collège du renseignement.

Le Comité R estime qu'il s'agit d'une première approche de cette problématique. Il a l'intention d'ouvrir une enquête de contrôle qui portera sur le "renseignement économique".

CHAPITRE 6 : CONTACTS DU COMITE R AVEC LE BVD ET LE MID ⁽¹⁾

Le 12 février 1997, le Comité R a reçu une délégation du BVD et du MID.

Cette délégation se composait du Chef adjoint et du Chef de cabinet du BVD. Le MID était quant à lui représenté par le Général de brigade, Chef du MID, par le Chef d'Etat-major ainsi que du Chef du Service de Contre-ingérence et de la sécurité.

La présidente, les membres, le greffier et le chef du service d'Enquêtes du Comité R étaient présents.

Un membre du Comité R a fait un exposé sur la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et sur le règlement d'ordre intérieur du Comité R. Cet exposé a été suivi d'un débat.

Les invités ont manifesté un grand intérêt pour la législation belge et, en particulier, pour le fonctionnement du Service d'enquêtes. Les dispositions prévues dans le règlement d'ordre intérieur pour garantir la confidentialité des données dont la diffusion pourrait entraver le fonctionnement des services de renseignement nationaux et étrangers, ont retenu toute leur attention.

Ensuite, la délégation néerlandaise et le Comité R ont été reçus au Parlement par les Commissions spéciales chargées du suivi parlementaire des Comités permanents de contrôle des services de police et de renseignement.

Les membres du Parlement se sont intéressés au fonctionnement des services de renseignement néerlandais, à la collaboration qu'ils entretiennent entre eux ainsi qu'à leur collaboration avec d'autres services.

Pendant ces échanges de vues, le BVD et le MID ont fourni des explications sur la réglementation en vigueur, sans toutefois aborder les sujets opérationnels.

Le Comité R a, à son tour, rendu visite aux Pays-Bas tant au BVD qu'au MID.

Ces contacts ont permis au Comité R de compléter son étude sur la législation relative aux services de renseignement et de sécurité néerlandais.

⁽¹⁾ BVD : Binnenlandse veiligheidsdienst - service de renseignement civil des Pays -Bas.
MID : Militaire inlichtingendienst - service de renseignement militaire des Pays -Bas.

CHAPITRE 7 : COLLOQUE “TERRORISME ET PROLIFÉRATION”

S'il est deux sujets importants auxquels les services de renseignement doivent être particulièrement attentifs à notre époque, c'est bien ceux du terrorisme et de la prolifération des armes. C'est la raison pour laquelle le Comité R a délégué un de ses membres pour assister à cet intéressant colloque, organisé par l'Institut Royal Supérieur de Défense le 5 mars 1997. Le Comité R a noté avec satisfaction que le SGR y avait également délégué plusieurs de ses membres.

Sept éminents spécialistes européens se sont succédé à la tribune :

Messieurs H. Muller, directeur de recherche au *Peace Research Institute* de Frankfurt et J. Krause, directeur adjoint de la *Deutsche Gesellschaft für Auswärtige Politik* ont présenté les risques liés à la prolifération de l'armement conventionnel et des armes de destruction massive dans différentes parties du monde. Messieurs F. Géré, maître de recherche au *Centre de recherche sur les stratégies et les technologies (CREST)* à Paris, et P. Wilkinson, professeur à l'Université de St Andrews (GB) ont présenté les options politiques de l'Europe occidentale en matière de lutte contre le terrorisme et la contre-prolifération.

Deux représentants du monde politique européen ont fait part d'expériences personnelles vécues dans l'exercice de leurs mandats alors qu'ils étaient confrontés à des problèmes de terrorisme.

Monsieur Baron Crespo, ancien ministre du gouvernement espagnol, ancien président du Parlement européen, membre de la Commission des Affaires étrangères, de la sécurité et de la politique de défense de l'Union européenne a parlé du terrorisme de l'ETA.

Monsieur Michel Rocard, ancien Premier ministre de la République française, membre du Parlement européen, membre de la Commission des Affaires étrangères, de la sécurité et de la politique de défense de l'Union européenne a dressé l'inventaire des traités internationaux en matière de prolifération. Il a également expliqué la manière dont il avait traité les problèmes de terrorisme en France lorsqu'il était Premier ministre.

Monsieur J. Truyens, chercheur à l'Université de Gand, a effectué la synthèse du colloque.

Résumer ici en quelques lignes les différents exposés entendus lors de ce colloque serait prendre le risque de les trahir. Le Comité R retiendra particulièrement l'importance du rôle que Michel Rocard reconnaît aux services de renseignements dans le traitement politique du terrorisme. Selon lui, il faut toujours laisser une porte entrouverte à la négociation. Mais pour cela, il faut savoir avec qui il est possible de négocier. Il faut aussi accepter de prendre des risques; et Michel Rocard de citer en exemple les négociations secrètes qu'il a organisées à Paris avec des représentants du FNLKS (organisation indépendantiste de Nouvelle Calédonie), alors que ceux-ci étaient tous recherchés par la police et sous le coup de mandats d'arrêt.

Michel Rocard regrette aussi le manque de considération que la culture latine accorde à la fonction du renseignement. Chez nous, dit-il, cette fonction est perçue avec méfiance; dans les pays anglo-saxons, on l'appelle "intelligence". Chez nous, la carrière professionnelle des membres des

services de renseignements n'est guère valorisée; dans les pays anglo-saxons, on y recrute les universitaires les plus brillants.

CHAPITRE 8 : CONGRES INFOWARCON A BRUXELLES

Le congrès InfoWARCon s'est tenu à Bruxelles les 7, 8 et 9 mai. Il était organisé par l'association américaine "NATIONAL COMPUTER SECURITY ASSOCIATION" (NCSA). Cette conférence, également appelée "WAR BY OTHER MEANS" a été sponsorisée par entre autres Winn Schwartau (Interpac, Inc.) et Robert Steele (OPEN SOURCES SOLUTIONS, Inc.).

Winn Schwartau est aux Etats Unis un des experts les plus renommés dans le domaine de la sécurité de l'information. Il est aussi écrivain ⁽¹⁾.

Robert Steele, un ancien agent de la CIA, est actuellement considéré comme une sommité dans la problématique de l'utilisation d'ordinateurs comme armes contre des individus ou des organisations. Il soutient notamment que même des systèmes informatiques réputés sûrs, sont vulnérables aux attaques de terroristes ou de puissances ennemies ⁽²⁾.

Un membre du Comité R a assuré la présidence d'honneur de ce congrès. Ce membre a aussi apporté sa contribution au congrès, notamment en y faisant participer des orateurs européens, ceci afin de lui donner une "perspective plus européenne".

Le but de ce congrès était de créer une prise de conscience de tous les dangers liés à l'évolution rapide du monde de l'électronique. Les milieux militaires, gouvernementaux, industriels ou policiers ne sont pas encore prêts à faire face sérieusement aux diverses sortes d'attaques dirigées contre leurs réseaux d'ordinateurs.

Des membres des services de renseignement ainsi que des services de police assistaient à ce congrès.

Pour Winn Schwartau, il n'existe aucun doute, "*la troisième guerre mondiale est en cours*". Il désigne ainsi la lutte économique que se livrent l'Occident et surtout les pays asiatiques comme la Chine, ... qui piratent les systèmes d'ordinateurs américains et ouest-européens pour s'approprier leurs "savoir-faire".

Suivant son compatriote Robert Steele, la Belgique est particulièrement mal engagée dans ce conflit mondial : "*Believe me, Belgium is skating on thin ice*" ⁽³⁾. Pas une seule institution belge ne protège suffisamment ses systèmes informatiques, pense Steele. Un incident grave peut survenir à tout moment. Ceci dit, Steele pense que les Etats-Unis ne sont pas beaucoup mieux lotis. Seulement, personne ne veut le savoir. Nous sommes tranquillement assis à attendre un "Pearl Harbor" électronique ou un "Chernobyl" informatique" ⁽⁴⁾.

⁽¹⁾ Voir chapitre 1. - Congrès de Washington

⁽²⁾ Traduction libre

⁽³⁾ "*Croyez-moi, la Belgique patine sur une glace fragile*"

⁽⁴⁾ Voir Knack Extra des 4-10 juin 1997 - p. 35

John Fialka, journaliste au Wall Street Journal, constate clairement qu'aucune loi ne nous protégera tant que les législateurs ne se sentiront pas concernés par ces préoccupations. Aussi longtemps que les victimes ne reconnaîtront pas avoir été volées ou sabotées, le milieu des affaires ne prendra aucune mesure pour se protéger. Cela s'appelle dans un autre domaine le "rape victim syndrom" ⁽⁵⁾. L'illusion est que si on tait le problème, il disparaîtra de lui-même. Mais voilà, le problème ne disparaît pas si facilement. ⁽⁶⁾.

Matthew Warren ⁽⁷⁾, qui étudie la matière à la "Portsmouth Business School", cite un rapport du Département de la Défense nationale des Etats-Unis d'où il ressort qu'en 1996, 250.000 tentatives d'effraction se sont produites dans les ordinateurs militaires, dont 162.500 avec succès. La plupart de ces attaques ne provenaient pas de terroristes ou de criminels. Matthew Warren pense que si les ordinateurs militaires courent un risque, les réseaux civils sont des cibles encore plus vulnérables. Les réseaux privés ont des degrés de sécurité très variables. Ils deviendront des cibles intéressantes pour les terroristes. Matthew Warren est persuadé que les "attacks" ne tarderont pas à venir. On peut déjà déstabiliser une entreprise en lui adressant des milliers de courriers électroniques ("E-mails") ⁽⁸⁾.

Divers orateurs ont exposé d'autres exemples d'attaques électroniques contre des banques ou contre des sociétés. Même s'ils semblent tirés de la science-fiction, il s'agit malheureusement de cas réels.

Plusieurs orateurs belges sont intervenus à leur tour et ont montré que cette nouvelle forme de criminalité ne peut pas être combattue en appliquant tel quel notre droit pénal actuel. Notre pays ne dispose toujours pas d'une législation spécifique pour combattre la criminalité informatique.

Internet est une invention remarquable, mais ce réseau est également utilisé pour commettre des crimes graves tels que l'espionnage économique, le blanchiment d'argent, la diffusion de pornographie infantine, etc...

Comme cette criminalité se joue des frontières, les nombreux problèmes juridiques qui se posent ne peuvent plus être résolus dans le seul cadre d'une législation nationale, ni même européenne. Une législation et des règles de procédure internationales sont nécessaires pour éviter qu'on abuse impunément des "autoroutes de l'information" et qu'on aboutisse ainsi à un chaos absolu.

En attendant cette réglementation internationale, un premier pas significatif serait, selon Robert Steele, de fixer au moins un standard international de protection des ordinateurs. *"Pour l'instant, ajoute-t-il, aucun fournisseur de matériel, ni de software, ni de hardware, ne peut être rendu responsable de la sécurisation de ses produits. Qu'un ordinateur soit piraté ? Pas de chance, dira-t-on : aucun des fournisseurs ne peut être rendu responsable. C'est pourquoi l'exigence d'un tel standard international doit être notre première préoccupation"*, dit encore Steele ⁽⁹⁾.

⁽⁵⁾ syndrome de la victime violée

⁽⁶⁾ Traduction libre - Computing du 22 mai 1997 - p. 22

⁽⁷⁾ Le docteur Warren est "Head of the Business Security Group", Plymouth University, U.K.

⁽⁸⁾ Traduction libre - Computing du 22 mai 1997 - p. 22

⁽⁹⁾ Voir Knack Extra des 4-10 juin 1997 - p. 35

CONCLUSIONS

Le Comité R est conscient que les problèmes propres à ce monde nouveau de l'électronique ne peuvent être résolus que dans la mesure où les autorités politiques en prennent conscience et aient la volonté d'agir en la matière.

Le Comité R se réfère ici aux conclusions de trois orateurs, à savoir Messieurs Oosterlinck, recteur de l'Université Catholique de Leuven (K.U.L.), Guy Maréchal, "Senior Adviser for the Information Security" chez Philips, et le professeur Bart De Schutter de la "Vrij Universiteit van Brussel" (V.U.B.).

- Le recteur Oosterlinck

Selon lui, l'histoire enseigne que les nouvelles technologies sont toujours utilisées sur les champs de batailles internationaux. Il y a peu de raisons d'attendre d'une "cyberwar" quelque chose de fondamentalement différent d'une guerre traditionnelle.

Les causes, les acteurs principaux, les moyens les plus importants et le déroulement des guerres futures seront bien entendu influencés par la mise en oeuvre de l'informatique, mais ils n'en seront pas essentiellement modifiés.

Voilà pourquoi le ton affolé d'une grande partie de la littérature concernant la "cyberwar" n'est pas justifié. Il est exact que les moyens informatiques imparfaits dont nous disposons à l'heure actuelle présentent un certain nombre de talons d'Achille. Mais il existe différents moyens de défense, suivant la nature des "attaques".

Sur le plan légal, nous avons besoin de nouveaux instruments, en évitant toutefois de créer un carcan légaliste excessif sur Internet, ce qui serait contraire à l'esprit même de ce réseau. La recherche cryptographique est donc essentielle pour faire d'Internet un instrument largement utilisable à des multiples fins. D'autres aspects de la technologie de l'information méritent une étude plus approfondie et plus raffinée.

Il y a actuellement des motifs de préoccupation, mais pas de panique. L'information est à la fois un moyen et un but pour les plans militaires. L'information est en fin de compte ce qui fait marcher une armée, une industrie, une entreprise, une université ou quoi que ce soit d'autre. Une information bien organisée renforce les liens de collaboration entre les hommes, et rien que pour cette raison, l'information et la technologie de l'information sont déjà stratégiquement intéressantes.

De là, la nécessité de rester attentifs à ces nouvelles technologies au moyen desquelles on peut construire un monde meilleur, mais aussi le détruire d'une manière plus fondamentale.

Nous avons le devoir de prévenir ce danger et de tout mettre en oeuvre pour l'empêcher, sans pour autant provoquer une panique aveugle en échafaudant des scénarios de guerre futuristes mais irréalistes.

- Guy Maréchal.

Pour lui, les éléments de base pour organiser démocratiquement la sécurité informatique dans la société de l'information semblent être identifiés; il existe des exemples de leur application. Les technologies nécessaires à cette fin sont disponibles à un prix abordable. La véritable question est de savoir si nos autorités politiques et si les personnes privées sont prêtes à jouer leur rôle pour l'organiser de manière fiable et démocratique.

- Le professeur De Schutter.

Selon lui, les secteurs public et privé doivent en tout état de cause, suivre attentivement l'évolution législative en cours. Ils doivent susciter un dialogue de coopération avec le législateur afin de s'assurer que les points de vue des producteurs, des "providers" et des usagers soient représentés. Ce dialogue devra finalement déboucher sur un consensus acceptable, représentatif d'un juste équilibre entre tous les intérêts en cause ⁽¹⁰⁾.

⁽¹⁰⁾ Traduction libre des conclusions des trois orateurs.

TITRE IV : EVOLUTION DU COMITÉ

1. LA COMPOSITION DU COMITÉ R

Etant donné que le vice-président du Comité R, qui a démissionné en novembre 1995, n'a pas encore été remplacé à ce jour, le Comité R a poursuivi son travail cette année encore avec quatre membres au lieu des cinq membres prévus par la loi.

Le Service d'enquêtes du Comité R ne dispose pas davantage du cadre complet de cinq unités. Actuellement, il y a trois enquêteurs dont un chef faisant fonction.

Le 3 juillet 1997, le Comité R a retenu la candidature d'un premier substitut du Procureur du Roi de Bruxelles pour la fonction de chef du Service d'enquêtes. Dès sa nomination, le nombre d'enquêteurs sera ainsi porté à quatre.

La composition du personnel administratif a connu peu de changements en comparaison avec le rapport annuel de l'année dernière.

Un employé stagiaire est passé sous statut et, la commission de comptabilité de la Chambre des Représentants a donné son accord pour l'engagement d'un agent temporaire pour scanner le fichier de documentation. Cet agent vient d'être recruté.

Le Parlement a fixé comme suit le cadre du personnel administratif : cinq agents sous statut et un militaire "occupé hors du cadre des forces armées".

Le cadre effectif se compose actuellement de :

- un comptable sous statut;
- une secrétaire sous statut;
- une employée sous statut;
- une employée détachée du Ministère de la Justice;
- un chauffeur-technicien détaché de l'Armée;
- un militaire (hors cadres) chargé de l'accueil;
- un employé temporaire pour la documentation (sous contrat de courte durée) .

2. LES ACTIVITÉS DU COMITÉ

Le lien étroit qui existe entre les deux Comités permanents et l'existence de réglementations d'ordre pratique, résultant essentiellement de l'installation des institutions dans un bâtiment commun, nécessitent une coordination permanente au niveau logistique.

Dans le fonctionnement journalier, cette coordination est essentiellement réglée par les greffiers des deux Comités permanents. Ainsi, par exemple, les services de réception, de téléphonie et de messagerie sont assurés en commun. Des cours de français et de néerlandais ont notamment été organisés.

Comme le mentionne déjà le rapport annuel précédent, la concertation a été également nécessaire pour mener une enquête commune. La même enquête a été poursuivie cette année et a donc à nouveau été un sujet abordé au cours des réunions communes avec tous les membres des deux Comités permanents.

Au cours de ces réunions (au cours de la période mentionnée, il y en a eu quatre), des problèmes de principes ont également été abordés tels que la concordance des procédures internes avec les exigences de la protection de la vie privée.

D'autre part, on discuta de projets visant à réduire les dépenses.

3. LES MOYENS FINANCIERS

Le Parlement a approuvé pour l'exercice 1996 une dotation d'un montant de 72.730.000 BEF. Le dernier exercice a été clôturé avec un montant de dépenses total de 49.315.450 BEF.

Le boni, 23.414.550 BEF, est mis, comme les années précédentes, à la disposition du Parlement.

Pour l'exercice 1997, le Comité R dépose une proposition pour un montant total de : 72.415.000 BEF. Le parlement⁽¹⁾ a amendé cette proposition de manière limitée en approuvant la création d'un fond social pour le personnel, qui aurait été alimenté par les intérêts financiers et en réduisant le poste "impôts et précompte immobilier".

Par le transfert du boni de 1995 (22.100.000 BEF) à l'exercice 1997, la dotation pour 1997 est réduite d'un même montant pour 1997 sur le plan comptable.

Le montant total disponible du budget 1997 est de 70.715.000 BEF.

Le Comité R partage sans réserve⁽¹⁾ l'avis que les propositions budgétaires doivent être également discutées par les commissions parlementaires d'accompagnement et que, dans l'attente d'éventuelles modifications législatives, les crédits doivent être maintenus.

Le Comité R estime rassurant que la Cour des Comptes ait été chargée d'effectuer un contrôle des comptes des Comités permanents P et R et d'en établir un rapport à l'intention du Parlement. Les organes de contrôle doivent être également contrôlés⁽¹⁾.

(1) Document 815/1 - 96/97 - Chambre des Représentants - p. 14 et suivantes

(2) Idem p. 10

(3) Lettre du 16 décembre 1997 du Président de la Chambre des Représentants aux Comités permanents P et R

4. ACTIVITÉS COMMUNES AVEC LE COMITÉ P

Le lien étroit qui existe entre les deux Comités permanents et l'existence de réglementations d'ordre pratique, résultant essentiellement de l'installation des institutions dans un bâtiment commun, nécessitent une coordination permanente au niveau logistique. Dans le fonctionnement journalier, cette coordination est essentiellement réglée par les greffiers des deux Comités permanents. Ainsi par exemple, les services de réception, de téléphonie et de messagerie sont assurés en commun. Des cours de français et de néerlandais ont notamment été organisés.

Comme le mentionne déjà le rapport annuel précédent, la concertation a été également nécessaire pour mener une enquête commune. La même enquête a été poursuivie cette année et a donc à nouveau été un sujet abordé au cours des réunions communes avec tous les membres des deux Comités permanents.

Au cours de ces réunions (*au cours de la période mentionnée, il y en a eu quatre*) des problèmes de principe ont également été abordés tels que la concordance des procédures internes avec les exigences de la protection de la vie privée.

En outre, il a été discuté de projets visant à régler les dépenses.

TITRE V : RECOMMANDATIONS

BILAN 1997 DE QUATRE ANNÉES DE CONTRÔLE ET DE RECOMMANDATIONS

Après quatre premières années de contrôle et de recommandations, le Comité R dresse ici un bilan :

- de ses principales constatations et recommandations;
- des réformes en projet ou réalisées dans le fonctionnement des services de renseignement;
- des améliorations qui doivent encore être apportées en vue d'une protection accrue des droits des citoyens et de l'efficacité de ces services.

Conformément à ses missions légales, les préoccupations du Comité R ont porté sur les points suivants :

- l'adoption d'une loi organique sur les services de renseignement incluant une définition claire de leurs missions et de leurs méthodes;
- la protection des droits des citoyens par un contrôle strict des méthodes employées;
- l'efficacité, la coordination et la collaboration de ces services.

Dans cet esprit, le Comité R s'est intéressé aux législations étrangères relatives aux services de renseignement, notamment aux législations de la République fédérale d'Allemagne, des Pays-Bas, du Portugal, de la Suisse, du Grand-Duché de Luxembourg, de la France, du Royaume-Uni, d'Italie, des Etats-Unis et du Canada.

A partir de ce bilan, le Comité souhaite mener une réflexion approfondie sur ce que les services de renseignement devraient être en tenant compte de la balance des intérêts qu'il convient de faire entre la protection des droits des citoyens et l'efficacité de ces services.

1. UNE LOI ORGANIQUE SUR LES SERVICES DE RENSEIGNEMENT

Les conclusions et recommandations principales du rapport d'activités de 1994 étaient :

“Le Comité estime essentiel qu'un texte de loi spécifique soit adopté pour fixer et réglementer aussi bien les missions que les méthodes des services de renseignements. (...) A défaut d'un texte de loi spécifique, les méthodes des services de renseignements n'offrent aucune sécurité juridique pour les citoyens, qui ne sont pas protégés contre d'éventuelles ingérences abusives de ces services dans leur vie privée. (...) Un texte de loi donnant un statut complet à ces services contribuerait aussi à améliorer leur efficacité”.

Une telle loi donnerait aussi au Comité R la pleine mesure de sa mission de contrôle.

En 1995, le rapport d'activités du Comité R analysait la note d'orientation du gouvernement concernant un avant-projet de loi relatif aux services de renseignement. Deux membres du Comité estimaient que la future loi devrait viser non seulement la Sûreté de l'Etat et le SGR, *“mais aussi tous les autres services (police, gendarmerie, etc...) dans la mesure où ils sont légalement habilités à recueillir, analyser et exploiter des renseignements de sécurité”*.

En 1995 également, faute de loi, le Comité R tentait de définir les missions des services de renseignement belges à travers les arrêtés royaux et les autres textes réglementaires en vigueur.

Le 2 juillet 1996, le gouvernement a déposé devant le Parlement un *“projet de loi organique des services de renseignement et de sécurité”*. Le Comité R a été invité par la commission mixte de la Chambre *“Justice - Défense nationale”* à remettre un avis sur le projet de loi. Dans son avis remis à la commission le 7 janvier 1997, le Comité propose au Parlement d'ajouter un deuxième alinéa à l'article 2 de la future loi organique rédigé comme suit : *“Aucun autre service ne peut exécuter des missions de renseignement et de sécurité qu'en vertu d'une loi”*.

Le point de vue selon lequel la future loi doit viser tout service légalement habilité à remplir des missions de renseignement n'est pas partagé par le gouvernement : le projet de loi déposé ne vise que la Sûreté de l'Etat et le SGR. Certains parlementaires ont cependant déposé des amendements en vue d'élargir le champ d'application de la loi.

Au 30 juin 1997, le projet de loi était toujours en discussion au Parlement. Un vote est intervenu devant les commissions réunies de la Justice et de la Défense nationale de la Chambre des Représentants.

2. LA PROTECTION DES DROITS DES CITOYENS

2.1. Généralités

En 1994, le Comité R déclarait : *“A défaut d'un texte de loi spécifique, les méthodes des services de renseignements n'offrent aucune sécurité juridique pour les citoyens, qui ne sont pas protégés contre d'éventuelles ingérences abusives de ces services dans leur vie privée”*.

Analysant la note d'orientation du Gouvernement en 1995, le Comité R souhaitait que la définition des missions des services de renseignement ne soit pas trop large ou trop générale, *“car cela risquerait de leur donner un domaine d'intervention trop large à l'égard des libertés constitutionnelles et démocratiques”*.

Le projet de loi organique des services de renseignement et de sécurité indique que dans l'exercice de leurs missions, ces services veillent au respect et contribuent *“à la protection des libertés et droits individuels, ainsi qu'au développement démocratique de la société”*. Le 29 novembre 1995, la section de législation du Conseil d'Etat a cependant rendu un avis très sévère à ce propos sur ce projet de loi organique : elle reproche en effet au texte de reléguer au second plan la protection des droits fondamentaux dans une société démocratique. *“S'il peut être admis que l'autorité publique se dote de services dont la fonction spécifique consiste à lui fournir les renseignements propres à lui permettre de prévenir, par les décisions adéquates, les atteintes répréhensibles aux intérêts dont elle assume la responsabilité, il reste en effet que la loi doit aussi prémunir la collectivité contre le préjudice que pourraient, à la faveur du secret qui les caractérise habituellement, porter ces activités au libre exercice des droits fondamentaux”*.

2.2. Les enquêtes relatives à la protection des droits des citoyens

Le Comité R a toujours exercé sa mission de contrôle en tenant compte de la balance des intérêts qu'il convient de faire entre la protection des droits des citoyens et l'efficacité des services de renseignement. Cette préoccupation s'est surtout exprimée à travers les études et les enquêtes d'ordre général suivantes. Le droit individuel le plus souvent mentionné a été bien sûr le droit à la vie privée et familiale prévu par l'article 22 de la Constitution et l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales :

- *Les certificats de sécurité* (1995) : avec le Conseil d'Etat, le Comité R estime qu'aucune enquête portant sur la vie privée d'une personne et de sa famille ne peut être effectuée qu'en vertu d'une loi. Un droit de recours doit être accordé à la personne dont l'habilitation de sécurité est refusée ou retirée.
- *Les sectes nuisibles* (1995 et 1996) : il y a lieu bien sûr de traiter cette menace pour la vie civile sans porter atteinte à la liberté de conscience et à la liberté de culte reconnues par la Constitution.
- *La destruction de documents par la Sûreté de l'Etat et le SGR* (1995) : une des questions posées dans cette enquête était notamment : comment la Commission de protection de la vie privée et le Comité R pourraient-ils accomplir leurs missions de protection des droits des citoyens si les services de renseignement pouvaient, sans autre forme de procès, détruire les données personnelles qu'ils détiennent.
- *Les statuts des agents des services de renseignement* (1996 et 1997) : l'agrégation préalable des candidatures par le ministre à un emploi dans les services de renseignement, est-elle conforme aux articles 10, 11 et 22 de la Constitution ? Le Comité R estime aussi que les agents des services de renseignement doivent jouir des mêmes garanties que celles dont jouissent les agents de l'Etat en matière d'évaluation et de procédure disciplinaire. Ils doivent également jouir de droits syndicaux compatibles avec leur fonction.
- *Les droits d'accès du particulier à son dossier individuel auprès d'un service de renseignement* (1997) : le Comité R estime qu'une personne qui fait état d'un préjudice matériel ou moral vraisemblable en rapport avec des informations contenues sur elle dans un dossier des services de renseignement devrait pouvoir obtenir, sous certaines conditions mais de manière plus large qu'aujourd'hui, un droit de consulter ces documents. L'opportunité de permettre ou de refuser cet accès ne doit pas être laissée à la seule appréciation des services de renseignement.
- *L'interception des télécommunications, les écoutes de sécurité* (1996 et 1997) : les prohibitions légales en la matière sont bien sûr motivées par le respect dû à la vie privée et familiale des citoyens. Le Comité préconise de revoir la législation pour permettre le recours aux écoutes de sécurité, mais avec de solides garanties de contrôle et de recours pour le citoyen.

En attendant le vote d'une loi autorisant les services de renseignement à procéder à des interceptions de sécurité, le SGR a volontairement remis au Comité R les appareils d'écoutes dont il disposait et qui permettaient de procéder à de telles interceptions.

- *les activités du SGR, la constitution de cellules provinciales par ce service* (1997) : cette enquête a été ouverte, entre autres, sur demande du ministre de la Défense nationale qui souhaitait vérifier les assertions selon lesquelles le SGR espionnait des civils à partir de ses postes

provinciaux.

- *La création éventuelle d'un nouveau service de renseignement spécialement chargé de surveiller les immigrés (1997)* : la presse et le monde politique ont quasi unanimement condamné un passage d'une note destinée à l'Etat-major des forces armées dont le contenu était jugé raciste. Le Comité R a enquêté pour voir en quoi le SGR ou un éventuel nouveau service de renseignement était ou non impliqué dans la rédaction et dans la mise en oeuvre de cette note.

Par ailleurs, le Comité R a aussi enquêté et fait rapport sur cinq plaintes introduites par des particuliers : aucune enquête n'a conclu à un préjudice disproportionné ou injustifié aux droits et libertés des plaignants.

3. L'EFFICACITÉ DES SERVICES DE RENSEIGNEMENT

Pour le Comité R, l'efficacité des services de renseignement est conditionnée tout à la fois :

- par une définition claire de leurs missions et un choix responsable de leurs objectifs; leurs activités doivent s'inscrire dans un contexte tant national qu'international;
- par la possibilité de recourir légalement mais de manière contrôlée à certaines méthodes spéciales de recherche du renseignement.
- par l'octroi d'un budget permettant aux services de remplir les missions qui leur ont été assignées;
- par la mise à leur disposition d'un personnel suffisant, qualifié et bénéficiant d'un statut garanti;
- par une structure et une organisation adaptées aux missions actuelles des services;
- par une définition raisonnable et adaptée du secret (secret professionnel, secret des sources, secret de l'information, etc ...);
- par une coordination des activités des services de renseignement et une collaboration effective entre ces services et les services de police.

3.1. La définition des missions des services de renseignement

Le projet de loi organique des services de renseignement contient, comme le souhaite le Comité R, une définition générale des missions de la Sûreté de l'Etat et du SGR.

3.1.1. Les missions de renseignement

a) La liste des sujets

Jusqu'à ce qu'une loi organique définisse les missions générales des services de renseignement, ces derniers n'auront pour base de travail qu'une "liste des sujets". En 1995, le Comité R demandait cette "liste des sujets" sur laquelle travaille la Sûreté de l'Etat soit régulièrement soumise au ministre de la Justice pour qu'il l'approuve personnellement.

“Les critères permettant de faire figurer une organisation ou un groupe sur la liste des sujets doivent être définis”.

La liste des sujets de la Sûreté de l'Etat du 14 octobre 1996 contient à présent une note préalable exposant les activités et les critères qui déterminent les personnes et les organisations qui y figurent. Les finalités des traitements de données sont aussi indiquées. A la connaissance du Comité R, la liste n'est cependant pas encore signée par le ministre de la Justice.

La liste des sujets du SGR n'indique pas encore les critères qui président à sa confection. A la connaissance du Comité R, la liste n'est pas non plus approuvée par le ministre de la Défense nationale.

Il faut toutefois noter que l'article 3 de l'arrêté royal du 21 juin 1996 portant création d'un Comité ministériel du renseignement et de la sécurité confie à cette instance la mission d'établir la politique générale du renseignement et de déterminer les priorités des services de renseignement. Cette disposition établit donc une responsabilité ministérielle collégiale en la matière.

Le Comité R estime, quant à lui, que cette responsabilité collégiale ne peut affecter la responsabilité individuelle des ministres compétents qui doit être engagée sous peine de voir cette responsabilité se diluer.

Le Comité a appris que le ministre de la Défense nationale avait entrepris les entretiens nécessaires pour prendre cette responsabilité par écrit.

b) les sectes

Parmi les nouveaux sujets devant intéresser les services de renseignement, le Comité R a cité dès 1995 les sectes nuisibles. En 1996, le Comité R recommandait une meilleure collaboration sur ce sujet entre la Sûreté de l'Etat et le SGR, en vue d'une politique commune dans le domaine des certificats de sécurité. Il préconisait aussi une large diffusion du renseignement sur ce sujet.

La commission chargée de l'enquête parlementaire *“visant à élaborer une politique en vue de lutter contre les pratiques illégales des sectes et le danger qu'elles représentent pour la société et pour les personnes, particulièrement les mineurs d'âge”* estime quant à elle *“qu'une amélioration de la coordination s'impose entre les différents services de police et de renseignement, ainsi qu'entre ces services et les autorités judiciaires”* ⁽¹⁾. La commission préconise notamment *“la consécration du rôle de la Sûreté de l'Etat, qui doit être chargée, en coordination avec tous les autres services de renseignement et de police, d'une activité de collecte, de centralisation et surtout d'analyse de l'information”*.

Le protocole d'accord signé en mai 1997 par le SGR et la Sûreté de l'Etat met cette recommandation en oeuvre en ce qui concerne les services de renseignement.

Le projet de loi organique des services de renseignement et de sécurité confirme que *“la contrainte morale ou physique exercée par une organisation à caractère sectaire”* est une menace contre *“la sûreté intérieure de l'Etat et la pérennité de l'ordre démocratique et*

⁽¹⁾ Chambre des représentants - 313 / 8 - 95 / 96 - 28 avril 1997, p.221.

constitutionnel” dont la Sûreté de l’Etat doit s’occuper.

c) Les nouvelles missions de renseignements

Le projet de loi organique des services de renseignement et de sécurité définit de nouvelles missions de renseignement, notamment :

- la sûreté extérieure de l’Etat et les relations internationales;
- l’activité qui menace ou pourrait menacer la sécurité des ressortissants belges à l’étranger;
- la sauvegarde du potentiel scientifique ou économique du pays.

Le Comité R a, à plusieurs reprises depuis 1995, souligné l’importance de ces missions. Toutefois, il ne peut que constater qu’à défaut de moyens supplémentaires en personnel qualifié, les services de renseignement seront dans l’impossibilité de remplir ces nouvelles missions.

3.1.2. Les missions de sécurité

Sur ce plan, le Comité R estimait aussi en 1994 que *“la loi devrait (...) définir le rôle attendu des services de renseignement en matière de sécurité”*. En 1995 et 1996, le Comité R a consacré plusieurs enquêtes aux missions de sécurité des services de renseignement.

Dans chacun de ces sujets, le souci constant du Comité R a été d’attirer l’attention des autorités responsables sur l’importance des missions de sécurité afin de doter les services de renseignement de structures légales adéquates.

- *La sécurité des systèmes d’informations* : le Comité a encouragé les travaux du groupe Belinfosec; il a aussi relayé ses recommandations auprès du Parlement. Le protocole d’accord entre le SGR et la Sûreté de l’Etat prévoit une aide réciproque en ce domaine. Beaucoup reste cependant à faire sur le plan légal et réglementaire.
- *Les certificats de sécurité* : le gouvernement a élaboré deux avant-projets de loi, l’un relatif aux *“habilitations de sécurité”*, l’autre attribuant au Comité R la compétence de connaître des recours introduits contre des refus d’octroi de telles habilitations. Ces avant-projets ont été soumis au Conseil d’Etat; celui-ci a rendu ses avis les 21 et 28 mai 1997. Le Comité n’a pas encore eu l’occasion d’exprimer son avis sur ces projets mais il ne manquera pas de le faire prochainement.
- *La protection des personnes* : toute la section 2 du projet de *“loi organique des services de renseignement et de sécurité”* est consacrée à *“l’exercice des missions de protection des personnes”* par la Sûreté de l’Etat.
- *La conservation, l’archivage et la destruction des dossiers* : des directives claires existent à présent aussi bien à la Sûreté de l’Etat qu’au SGR. Un manque chronique de personnel administratif retarde cependant la mise en oeuvre de ces mesures dans les deux services de renseignement.

3.1.3. La diffusion du renseignement aux autorités politiques, administratives et judiciaires, ainsi qu'à des instances et à des personnes privées

Le Comité R estime que la diffusion du renseignement est une mission essentielle des services de renseignement. Analysant la note d'orientation du Gouvernement en 1995, le Comité R se demandait si le gouvernement devait être le seul destinataire des renseignements produits par la Sûreté de l'Etat. Le Comité pense en effet que les autorités des Communautés et Régions, voire même les gouverneurs de provinces et les bourgmestres devraient pouvoir bénéficier du renseignement en cas de nécessité.

La diffusion du renseignement a été débattue dans le cadre du § 3 de l'article 10 du projet de *"loi organique des services de renseignement et de sécurité"*. Des amendements ont été déposés en vue de permettre une large diffusion du renseignement, notamment aux services de renseignement et de sécurité étrangers, à des organes ou des personnes *"qui ont un motif légitime pour en prendre connaissance"*. Finalement, l'amendement n° 38 du gouvernement indique que *"les services de renseignement et de sécurité ne peuvent communiquer ces renseignements qu'aux ministres et aux autorités judiciaires et administratives concernés, aux services de police et à toutes instances et personnes déterminées conformément aux conditions définies par le Comité ministériel et aux finalités de leurs missions"*.

3.2. Les méthodes des services de renseignement

Le Comité R a toujours approuvé le principe général du projet de loi selon lequel les méthodes des services de renseignement doivent être exclusives de tout moyen de contrainte et ne peuvent, sauf cas exceptionnels porter atteinte à la vie privée; par conséquent :

- tout ce qui n'est pas interdit au citoyen est permis aux services de renseignement;
- une habilitation légale est nécessaire pour l'emploi de certaines méthodes particulières.

Ici aussi, le souci constant du Comité R a donc été d'attirer l'attention des autorités responsables sur l'importance pour les services de renseignement de pouvoir recourir de manière légale et contrôlée à certaines méthodes spéciales de recherche, notamment :

- l'utilisation d'informateurs;
- l'interception de télécommunications;
- l'interception de correspondance écrite;
- la pénétration et la fouille de lieux habités;
- la filature et l'observation de personnes, de réunions, de rassemblements;
- l'utilisation de moyens optiques de surveillance;
- le recueil de données à caractère personnel et l'accès à certains fichiers et informations détenus par d'autres autorités.

La nécessité d'une habilitation légale pour pouvoir recourir à ces méthodes ressort de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales. Le Comité R et le

Conseil d'Etat l'ont plusieurs fois soulignée.

Le Comité R s'est aussi intéressé à l'exploitation des "sources ouvertes" par les services de renseignement.

3.2.1. L'utilisation d'informateurs

Le présent rapport d'activités de 1997 contient une série de recommandations relatives à l'emploi de cette importante source d'informations pour les services de renseignement. Le Comité R recommande notamment que la législation applique en ce domaine les principes de la subsidiarité et de la proportionnalité. Il recommande aussi des directives claires de conduites et d'évaluation des informateurs ainsi que des mesures afin de garantir leur protection.

L'élaboration de toutes ces dispositions reste à faire.

3.2.2. L'interception de télécommunications

Ce sujet a plus d'une fois retenu l'attention du Comité R. En 1996, il a consacré un chapitre de son rapport d'activités à une étude théorique de la législation sur les écoutes administratives. En 1997, il a enquêté, à la demande du Parlement, sur les interceptions de télécommunications auxquelles procède le SGR.

Ce type d'activité est indispensable pour le SGR; elle est essentiellement orientée vers le domaine militaire et permet, entre autres, de déceler la présence - ou la disparition - de grandes unités. La section COMINT du SGR travaille en étroite collaboration avec les services alliés analogues dont elle reçoit également des renseignements indispensables

Actuellement, l'interception des télécommunications privées, même militaires, même à l'étranger, même en temps de guerre, est formellement prohibée par deux dispositions légales. Le Comité R a donc recommandé d'adapter la législation afin que le SGR puisse poursuivre cette mission dans un cadre légal. L'article 26 du projet de loi organique des services de renseignement y pourvoit partiellement.

Le Comité R sait par ailleurs qu'un avant-projet de loi sur les écoutes de sécurité est en cours d'élaboration en vue de permettre à la Sûreté de l'Etat d'y recourir. Dès que le Comité aura connaissance du contenu de cet avant-projet, il ne manquera pas de l'étudier.

3.2.3. L'accès à certains fichiers et informations détenus par d'autres autorités

En 1994, le Comité R constatait que de nombreux renseignements concernant des personnes étaient susceptibles d'être recueillis par une consultation de documents dressés et détenus par différents services publics. Ce recueil de renseignements s'effectuait surtout grâce à des contacts informels.

Analysant la note d'orientation de 1995, deux membres du Comité R estimaient que l'autorisation légale donnée aux fonctionnaires de communiquer des informations aux services de renseignement devait être limitée aux informations sollicitées par ces services, ceci en vue d'éviter des délations arbitraires. Ces deux membres concevaient toutefois d'accorder un droit de réquisition à l'égard de données détenues par des services de police, notamment dans le cadre du maintien de l'ordre

public, de la recherche de matières nucléaires et de la protection rapprochée de personnes. Deux autres membres proposaient quant à eux qu'un arrêté royal permette aux services de renseignement de consulter certaines banques de données de certains services publics.

L'article 10 du projet de loi organique des services de renseignement et de sécurité prévoit que les magistrats de l'ordre judiciaire, les fonctionnaires et les agents des services publics sollicités peuvent communiquer les informations demandées par ces services en se conformant à la loi *"et aux modalités déterminées par leurs autorités responsables"*.

Le Comité R s'est demandé à ce propos si le fait de laisser déterminer les modalités de communication par les autorités responsables n'engendrait pas un risque d'arbitraire de leur part. Le Comité a donc proposé que la communication d'informations par les fonctionnaires et les agents des services publics soit seulement "conforme à la loi", comme c'est le cas dans la législation néerlandaise.

Par ailleurs, le projet de loi prévoit que *"les modalités de communication des informations contenues dans les registres de la population et des étrangers sont fixées par arrêté royal délibéré en Conseil des ministres"*. Un amendement déposé par le gouvernement vise à instaurer le principe de la motivation d'un refus de communication des informations sollicitées par la Sûreté de l'Etat et le SGR. Le Comité R approuve ces dispositions.

L'article 7 du projet de loi relatif au casier judiciaire central prévoit notamment que *"les agents de niveau 1 des services de renseignements au sens de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, nommément désignés par écrit, (...) ont accès en permanence, uniquement dans le cadre de leurs missions prévues par la loi qui requièrent la connaissance du casier judiciaire, aux informations enregistrées dans le Casier judiciaire concernant chaque personne"* moyennant toutefois certaines exceptions. Ce texte a été adopté par la commission de la Justice le 15 juillet 1997 ⁽¹⁾.

Le Comité R approuve cette disposition en ce que seuls des agents nommément désignés par écrit seront habilités à avoir accès au casier judiciaire central. Une telle précaution est en effet de nature à limiter des abus qui pourraient être commis à l'occasion de la consultation de ce casier judiciaire central. Toutefois, en limitant cette prérogative aux seuls agents de niveau 1, le Comité R s'interroge sur les possibilités dont disposeront les militaires du SGR puisque leurs grades n'ont aucune équivalence avec les grades civils des agents de l'Etat.

3.2.4. L'exploitation des "sources ouvertes"

Depuis 1994, le Comité R est attentif à l'importance des "sources ouvertes" dans le monde du renseignement. En 1996, il a émis une proposition circonstanciée en vue d'une utilisation efficace des sources ouvertes par une unité commune des services de renseignement belges. La proposition comportait deux volets dans un premier temps :

1° élargir les services de documentation générale par l'engagement d'analystes;

2° la mise à la disposition des services de moyens informatiques suffisants.

⁽¹⁾ Chambre des représentants - 1 - 663 / 4 - s.o. 96 / 97, 15 juillet 1997, p. 5.

Le Comité R a plusieurs fois suggéré que le SGR et la Sûreté de l'Etat se raccordent ensemble à certaines banques de données commerciales pour réduire les coûts.

Les responsables des services de renseignement admettent que 80 à 90 % des informations nécessaires à leurs services peuvent à présent être trouvées au moyen de sources ouvertes. Cependant, des réticences subsistent quant à l'exploitation en commun de ces sources. Toutefois des contacts ont eu lieu entre ces services.

Le manque chronique de personnel administratif et d'analystes, ainsi que l'absence d'informaticien dans le cadre des services de renseignement constituent toutefois un frein au développement de cette ressource et à la collaboration des services dans ce domaine.

3.3. Les budgets des services de renseignement

En 1995, le Comité R a consacré un chapitre de son rapport d'activités aux budgets de la Sûreté de l'Etat et du SGR. Contrairement au SGR qui établit des prévisions budgétaires, la Sûreté de l'Etat n'a pas ce pouvoir, ce qui limite ses initiatives dans la programmation de ses missions. Par ailleurs, le Comité a recommandé que le SGR ne détruise plus systématiquement sa comptabilité comme il avait coutume de le faire. Cette recommandation a été suivie d'effets.

Le Comité R n'a plus mené aucune enquête sur ce sujet, ni en 1996, ni en 1997. Il ne manquera pas au cours de la prochaine année d'activités de vérifier l'emploi du budget accordé aux services de renseignement par rapport aux missions qui leur sont assignées.

3.4. Le personnel des services de renseignement

En 1996, le Comité R a entrepris l'étude des statuts des membres du personnel des services de renseignement. Le rapport d'activités de 1996 consacre un chapitre aux agents de la Sûreté de l'Etat, celui de 1997, aux agents du SGR.

Le souci du Comité en la matière est que les services de renseignement disposent d'un personnel stable, qualifié (notamment des juristes, des analystes et des informaticiens), en nombre suffisant et doté de statuts clairs et coordonnés. Le Comité a émis une vingtaine de recommandations visant à rapprocher les statuts spécifiques de ce personnel de celui des agents de l'Etat. Dans la mesure où certaines dispositions de ces statuts doivent rester spécifiques, elles doivent se rapprocher le plus possible les unes des autres; toute modification à l'un de ces statuts doit être apportée en concertation et, si possible en accord avec le ministre responsable de l'autre service.

Le Comité R a connaissance d'un projet d'arrêté royal relatif à la carrière des membres des services extérieurs de la Sûreté de l'Etat. Il sait aussi qu'une révision générale des barèmes a été décidée au ministère de la Défense nationale en 1994; certaines modifications au statut des agents civils du Service de sécurité militaire sont envisagées dans le cadre de cette révision générale des barèmes. A la connaissance du Comité R, ces projets sont examinés sans concertation entre les ministres compétents.

Le Comité R le regrette et il estime que cette concertation doit être mise sur pied sans tarder.

3.5. La restructuration et l'organisation des services de renseignement

Le Comité R s'intéresse à l'organisation et à la structure des services de renseignement depuis 1994.

Dans son premier rapport d'activités, il soulignait déjà que ces services avaient connu d'importants bouleversements :

- la scission en 1994 des deux services de l'Administration de la Sûreté publique (Office des étrangers et Sûreté de l'Etat);
- une réorganisation interne du SGR en 1993, laissant toutefois ce service sous l'autorité directe du chef de l'Etat-major général des forces armées.

En 1995, le Comité R émettait une série de recommandations relatives notamment à : l'élaboration, la mise à jour, le classement, la coordination, la codification et aux pouvoirs de signature des notes et ordres de service de la Sûreté de l'Etat. Le Comité R demandait aussi la rédaction simultanée des ordres permanents du SGR dans les deux langues nationales, ce qui a été fait depuis lors. En 1997, le Comité R a fait rapport sur la réinstallation des postes provinciaux du SGR.

La Sûreté de l'Etat a entrepris un travail de restructuration interne qui reste néanmoins inachevé malgré l'engagement de l'administrateur général de le mener à bien pour la fin de 1995. Un grand nombre de notes obsolètes n'ont pas encore été revues et il n'existe toujours pas de codification des ordres permanents applicables à la Sûreté de l'Etat.

En 1997, deux membres du Comité R ont proposé que la Sûreté de l'Etat dépende désormais du ministre de l'Intérieur plutôt que du ministre de la Justice, ceci pour trois raisons :

Tout d'abord, l'histoire des services de renseignement nous apprend que la Sûreté de l'Etat a été rattachée au ministre de l'Intérieur dans la seconde moitié du 19ème siècle.

Ensuite, les articles du projet de loi ne visent en aucun cas des activités relevant de la responsabilité ministérielle du ministre de la Justice. La Justice et le Renseignement sont deux matières distinctes l'une de l'autre.

Enfin, aucune loi des pays étudiés jusqu'à présent par le Comité R ne donne cette responsabilité au ministre de la Justice.

Le projet de loi organique des services de renseignement et de sécurité maintient quant à lui la Sûreté de l'Etat sous l'autorité du ministre de la Justice. Toutefois le ministre de l'Intérieur est associé à l'organisation et à l'administration de ce service en ce qui concerne l'exécution des missions de maintien de l'ordre public et de protection des personnes. Ainsi le ministre de l'Intérieur peut-il requérir la Sûreté de l'Etat pour ces missions, faire des recommandations et donner des indications précises sur les moyens à mettre en oeuvre et les ressources à utiliser.

A propos de ces pouvoirs, les deux membres précités du Comité R pensaient en 1995 :

- qu'une nouvelle loi conférant un droit de réquisition au ministre de l'Intérieur en matière de protection rapprochée restreindrait les compétences du Roi telles que fixées par l'article 11 de la loi du 5 août 1992 sur la fonction de police;
- que la prérogative accordée à ce ministre de faire des recommandations et de donner des indications précises sur les moyens à mettre en oeuvre et les ressources à utiliser était "*de nature à engendrer des conflits et des frustrations*" entre le ministre et le service concerné. Les deux membres précités préconisaient que ce pouvoir de recommandation soit plutôt accordé à un coordinateur.

De même, conformément à la note d'orientation, le projet de loi prévoit que la signature conjointe ou l'avis conforme du ministre de l'Intérieur est requis pour une série d'arrêtés réglementaires relatifs à la Sûreté de l'Etat. A ce propos, les deux membres précités pensaient que ces textes devraient plutôt être délibérés en Conseil ministériel du renseignement et de la sécurité.

A propos des dispositions du projet de loi opérant la répartition des compétences entre les ministres de la Justice, de l'Intérieur et de la Défense nationale, le Conseil d'Etat a estimé que c'est au pouvoir exécutif qu'il revient de régler son organisation et que le pouvoir législatif ne peut donc les adopter sans empiéter sur les pouvoirs que la Constitution réserve au Roi.

3.6. Une définition raisonnable et adaptée du secret

Une caractéristique essentielle des services de renseignement est de travailler dans le secret. Le Comité R s'est plusieurs fois interrogé sur la nature et le fondement de cette obligation de secret.

En 1995, c'est la manière dont la note d'orientation aborde le secret des sources et des informateurs qui retient l'attention du Comité R. Le problème est alors de trouver *“un équilibre entre la protection de l'anonymat des informateurs et la nécessité dans certains cas (devant la Justice) de connaître leur identité”*. En 1997, le Comité R a discuté de l'équilibre à trouver entre le droit d'accès du particulier à son dossier et la nécessité du secret.

Le Comité R est d'avis qu'en aucun cas, les services de renseignement ne peuvent rester seuls juges de l'obligation du secret :

- pour le témoignage en Justice, c'est la solution appliquée aux Pays-Bas qui est proposée : devant les juges, un membre d'un service de renseignement peut être dispensé de son devoir de secret moyennant l'accord de deux ministres, dont celui de tutelle.
- pour permettre ou refuser l'accès d'un particulier à son dossier auprès d'un service de renseignement, un organisme collégial tel que le Comité R, en accord avec le ministre compétent, pourrait constater que la communication de certaines informations ne met en cause ni la sûreté de l'Etat, ni la défense et la sécurité publique ni la sécurité de particuliers.

Le Comité R estime aussi qu'il conviendrait de définir dans la loi organique des services de renseignement et de sécurité, le secret de l'information elle-même, c'est-à-dire le contenu de l'information; la détermination des degrés de classification ne suffit pas.

Dans l'étude des statuts des membres des services de renseignement, le Comité R s'est penché brièvement sur les obligations de secret à laquelle ces agents sont tenus : il a décidé de consacrer une prochaine enquête à ce sujet.

3.7. La coordination des services de renseignement

3.7.1. La coordination des services de renseignement entre eux

En 1994, le Comité R déclarait : *“L'adoption d'une loi organique constituerait le cadre adéquat pour organiser la coordination des services de renseignements, aujourd'hui non structurée malgré de nombreuses zones d'intérêt et d'intervention commune”*. En 1995, le Comité R a regretté que les services de renseignement n'aient pas assuré la coordination de leurs activités de façon

systematique malgré le voeu du législateur. Le Comité déclarait toutefois que la responsabilité de ces services devait être nuancée dans la mesure où les ministres responsables n'avaient pas organisé cette coordination. Les principales recommandations du Comité R étaient donc :

- que l'établissement d'une politique en matière de renseignement et de sécurité se fasse au niveau du gouvernement et non des services;
- que l'établissement de la politique générale du renseignement et la fixation des priorités des services fasse l'objet d'une concertation collégiale au sein du gouvernement; il devait en être même pour la détermination d'une politique en matière de protection des informations sensibles.
- que, par contre, la fonction d'exécution et de coordination effective des missions opérationnelles des services de renseignement soit confiée à un "Coordinateur".

En 1995 et 1996, le Comité R a déploré des carences de coordination et d'échange d'informations entre le SGR et la Sûreté de l'Etat, notamment dans les enquêtes suivantes :

- enquête "*sur l'efficacité des services de renseignements relative à l'activité des sectes en Belgique*";
- enquête "*sur l'efficacité et la collaboration des services de renseignements à propos des événements du Rwanda*"

Deux arrêtés royaux du 21 juin 1996 ont créé le Comité ministériel du renseignement et de la sécurité d'une part, le Collège du renseignement et de la sécurité d'autre part : cette dernière instance a pour tâche de veiller à l'exécution coordonnée des décisions du Comité ministériel.

Enfin, un protocole d'accord a été signé le 20 février 1997 par l'administrateur général de la Sûreté de l'Etat et par le chef du SGR. Cet accord a été initié et approuvé par les ministres compétents. Le Comité R s'en réjouit mais il propose d'amender légèrement le protocole en ce qui concerne la lutte contre le crime organisé et la prolifération N.B.C., sujets dans lesquels le SGR devrait s'impliquer davantage. L'exécution pratique du protocole d'accord se met en oeuvre.

Par ailleurs, le projet de loi organique des services de renseignement fait obligation à ces services de coopérer de manière efficace.

3.7.2. La collaboration des services de renseignement avec les services de police

Le Comité R a plusieurs fois souligné que les services de police sont habilités à recueillir et à traiter des renseignements en vertu de l'article 39 de la loi sur la fonction de police.

En 1994, le Comité R estimait que le magistrat national pourrait, au sein d'un organe de concertation, assumer "*la nécessaire coordination entre les services de renseignements, les autorités judiciaires et les services de police concernés par les mêmes missions*".

D'autres mesures ont cependant été prises en vue d'assurer la coordination entre les services de renseignement et les services de police :

- d'une part, le fonctionnaire dirigeant de la Police générale du Royaume et le commandant de la Gendarmerie font partie du Collège du renseignement et de la sécurité (article 2 de l'arrêté royal du 21 juin 1996 portant création du Collège du renseignement et de la sécurité);

- d'autre part, le procureur général de Gand se voit confier la tâche spécifique des relations avec la Sûreté de l'Etat (article 3 de l'arrêté royal du 6 mai 1997 relatif aux tâches spécifiques des membres du collège des procureurs généraux).

Un amendement au projet de loi organique des services de renseignement et de sécurité fait à présent obligation aux services de renseignement d'assurer *“une collaboration efficace avec les services de police et les autorités administratives et judiciaires”*.

Le Comité estime quant à lui qu'à l'instar du protocole d'accord intervenu entre le SGR et la Sûreté de l'Etat, un tel protocole doit être signé entre les services de renseignement et les services de police. Un tel accord est nécessaire en vue de mettre en oeuvre la coordination prévue dans les textes légaux et réglementaires : celle-ci se justifie aussi en raison des matières de plus en plus nombreuses dans lesquelles les compétences de ces services se chevauchent, notamment le terrorisme, la criminalité organisée, le blanchiment d'argent, etc...

3.7.3. La dénonciation des crimes et délits aux autorités judiciaires

En 1994 déjà, le Comité R constatait que l'obligation de dénoncer tout crime et délit à l'autorité judiciaire prévue par l'article 29 du Code d'instruction criminelle, pouvait compromettre la poursuite des investigations des services de renseignement. En 1996 et en 1997, le Comité R a recommandé que cet article 29 soit amendé dans le sens du § 138 de la *“Strafprozessordnung”* de la République fédérale d'Allemagne. Cette disposition permet aux services de renseignement allemands d'apprécier la nécessité d'une communication d'un délit en fonction de sa gravité d'une part, de l'importance des opérations menées d'autre part. Les services de renseignement peuvent s'accorder avec le procureur général à cet égard. En 1997, le Comité R cite également en exemple l'article 22, alinéa 3 de la loi en vigueur aux Pays-Bas sur les services de renseignement et de sécurité qui prévoit lui aussi une concertation avec le ministère public.

Le projet de loi organique des services de renseignement et de sécurité ne contient aucune disposition modificative de l'article 29 du Code d'instruction criminelle.

Le Comité R espère pour sa part qu'un *“modus vivendi”* pourra être trouvé à ce sujet dans le cadre des organes de coordination cités ci-avant.