



**COMITE PERMANENT DE CONTROLE
DES SERVICES DE RENSEIGNEMENTS**

RAPPORT D'ACTIVITES

1999



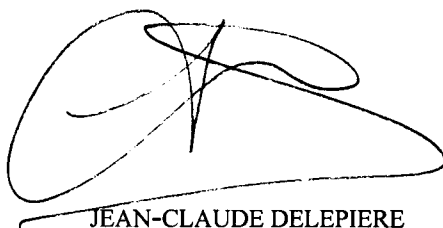
A Monsieur le Président du Sénat,
A Monsieur le Président de la Chambre des Représentants
A Monsieur le Ministre de la Justice,
A Monsieur le Ministre de la Défense nationale,

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 sixième rapport général d'activités.

Ce rapport couvre la période du 1^{er} août 1998 au 30 septembre 1999.

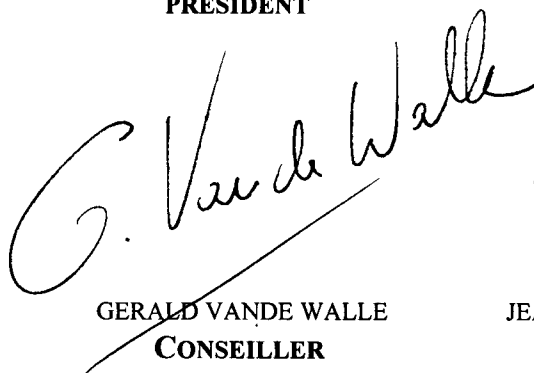
Nous vous prions de croire, Messieurs les Présidents, Messieurs les Ministres, en l'assurance de notre très haute considération.



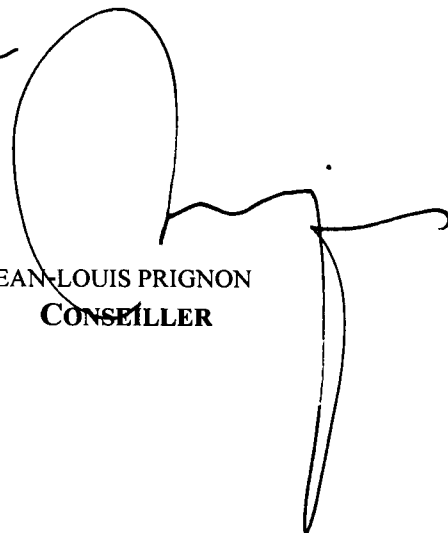
JEAN-CLAUDE DELEPIERE
PRESIDENT



DANIELLE CAILLOUX
CONSEILLER



GERALD VANDE WALLE
CONSEILLER



JEAN-LOUIS PRIGNON
CONSEILLER



WOUTER DE RIDDER
GREFFIER

TABLE DES MATIERES

TITRE I : ACTIVITES DU COMITE PERMANENT R APERCU ET PERSPECTIVES	-1-
ACTIVITES DU COMITE PERMANENT R	-2-
TITRE II : NOS SERVICES DE RENSEIGNEMENT	-12-
LES ENQUETES	
A. A LA REQUETE DU PARLEMENT OU DES MINISTRES	-12-
<u>Chapitre 1</u> : <i>Rapport de l'enquête sur la collecte de données par les services de renseignements à propos des parlementaires</i>	-13-
1. Introduction	-13-
2. Procédure	-13-
3. L'intérêt parlementaire	-14-
4. Les dossiers de la Sûreté de l'Etat	-15-
4.1. La constitution des dossiers en général	-15-
4.2. L'examen des dossiers des parlementaires	-16-
4.3. Les demandes de consultation de dossiers individuels introduites par des parlementaires	-16-
4.4. Le jugement du Tribunal de Première Instance de Bruxelles du 5 décembre 1997	-17-
4.5. Destination des dossiers après examen et tri	-17-
5. Les dossiers du SGR	-18-
5.1. La constitution de dossiers sur les parlementaires	-18-
6. Conclusions générales	-19-
7. Recommandations	-19-

<u>Chapitre 2 :</u>	<i>Rapport relatif a une demande d'enquête émanant du député Olivier Deleuze, quant a l'interception supposée par la Sûreté de l'Etat de courrier dans le cadre d'une enquête judiciaire</i>	-20-
1.	Procédure	-20-
2.	L'intérêt parlementaire	-21-
3.	Déroulement de l'enquête	-21-
3.1.	Recherche des procès-verbaux	-21-
3.2.	Auditions	-21-
3.3.	Eléments du dossier du Parquet	-21-
3.4.	Les dossiers à la Sûreté de l'Etat	-22-
4.	Conclusions	-22-
<u>Chapitre 3 :</u>	<i>Rapport d'enquête sur la manière dont les services belges de renseignement réagissent face à l'éventualité d'un système américain "Echelon" d'interception des communications téléphoniques et fax en belgique</i>	-23-
1.	Introduction	-23-
2.	Procédure	-23-
3.	L'intérêt parlementaire	-24-
3.1.	Au niveau fédéral	-24-
3.2.	Au niveau Européen	-26-
3.3.	Le Parlement français	-28-
4.	Les sources ouvertes	-29-
4.1.	Zbigniew Brzezinski, ancien conseiller pour la Sécurité Nationale du Président Carter	-29-
4.2.	Amiral Pierre Lacoste, ancien directeur général de la "Direction générale de la Sécurité Extérieure" (France)	-30-
4.3.	Martin Brady, directeur du Defense Signals Directorate (DSD - Australie)	-30-
4.4.	Amendement à l'"Intelligence Authorization Act" (E.U.)	-31-
5.	Constatations à propos des services de renseignement belges	-31-
5.1.	A la Sûreté de l'Etat	-31-
5.2.	Au SGR	-32-
6.	Autres rapports rédigés pour le groupe STOA	-33-

7.	L'interception de communications par d'autres puissances que les Etats-Unis	-38-
7.1.	Espionnage : Alliance franco-allemande	-39-
7.2.	France : Opidium pour se défendre contre Echelon	-39-
7.3.	Ecoutes : Bientôt de grandes oreilles en Suisse	-40-
8.	Conclusions	-40-
9.	Recommandations	-41-
	Lexicon	-45-
B. A L'INITIATIVE DU COMITE R		-47-
<u>Chapitre 1 :</u>	<i>Rapport sur le suivi par le SGR des recommandations sur le Rwanda formulées par la commission d'enquête parlementaire</i>	<i>-48-</i>
1.	Motifs et objet de l'enquête	-48-
2.	Procédure	-48-
3.	Le suivi des différentes recommandations	-49-
3.1.	Les mesures prises par le SGR en matière de collecte du renseignement	-49-
3.2.	Les mesures prises par le SGR en matière d'analyse, d'évaluation et de diffusion du renseignement	-50-
3.3.	Le fonctionnement du SGR	-52-
3.4.	Autres mesures	-53-
4.	Conclusions	-54-
<u>Chapitre 2 :</u>	<i>Rapport sur la mise en application du "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".</i>	<i>-55-</i>
1.	Introduction	-55-
2.	Procédure	-55-
3.	Intérêt parlementaire	-56-
4.	Constatations	-56-

5. Recommandations	-57-
Chapitre 3 : <i>L'intervention de la Sûreté de l'Etat dans les procédures de naturalisation ainsi que dans le cadre de la loi sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers</i>	-59-
1. Introduction	-59-
2. Procédure	-60-
3. L'intérêt parlementaire	-60-
4. Historique des échanges d'informations entre l'Office des étrangers et la Sûreté de l'Etat	-61-
5. Les motifs d'échanges d'informations entre l'Office des étrangers et la Sûreté de l'Etat	-62-
5.1. Les Conventions internationales	-63-
5.2. L'échange d'informations en vue de l'application de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers	-64-
5.3. L'échange d'informations en vue de l'application de la loi du 28 juin 1984 relative à certains aspects de la condition des étrangers et instituant le Code de la nationalité belge	-67-
5.4. Les compétence de la Sûreté de l'Etat en matière d'armes à l'égard des étrangers	-69-
5.5. L'échange d'informations en vue de l'application de la législation relative à l'enseignement	-70-
6. Conclusions et recommandations	-70-
C. A L'INITIATIVE DU SERVICE D'ENQUÊTES	-73-
Enquête de contrôle relative à l'efficacité du SGR et à la collaboration des deux services de renseignement concernant le vol d'armes commis a Houthulst en 1997	-74-
1. Procédure	-74-
2. Motif de l'enquête	-74-
3. Normes en vigueur	-75-
3.1. "L'instruction sur la sécurité militaire" (IF 5)	-75-
3.2. Les "Directives Complémentaires de Sécurité" (DCS)	-78-

4.	Résumé de l'enquête	-78-
4.1.	Enoncé du problème	-78-
4.2.	Enquête à la suite du vol	-79-
4.3.	Les responsabilités pour la protection et la surveillance du dépôt de munitions	-79-
4.4.	Compétences du SGR en la matière	-80-
5.	Conclusions	-81-
6.	Recommandations	-82-
 D. LES PLAINTES		-84-
 <u>Chapitre 1</u> : <i>Enquête de contrôle relative a la plainte de monsieur X</i>		-85-
1.	Procédure	-85-
2.	Normes applicables à la problématique	-86-
3.	Synthèse de l'enquête	-87-
4.	Conclusions	-87-
 <u>Chapitre 2</u> : <i>Enquête de contrôle sur plainte de monsieur Y</i>		-88-
1.	Procédure	-88-
2.	Normes applicables à la problématique	-89-
3.	Synthèse de l'enquête	-90-
4.	Conclusions	-90-
 <u>Chapitre 3</u> : <i>Enquête de contrôle consécutive a la plainte déposée par monsieur Z</i> ..		-91-
1.	Procédure	-91-

2.	Résumé de l'enquête	-92-
2.1.	Audition du plaignant	-92-
2.2.	Examen du dossier conservé au SGR	-92-
3.	Constatations	-92-
4.	Conclusions	-93-
E. SUIVI DES ENQUETES DES ANNEES PRECEDENTES		-94-
<u>Chapitre 1 :</u>	<i>Echange de vues entre le comité permanent R et les services de renseignement et de sécurité à la suite d'une enquête de contrôle concernant les informateurs de la Sûreté de l'Etat et du SGR</i>	<i>-95-</i>
<u>Chapitre 2 :</u>	<i>Rapport relatif à l'échange de vues entre le SGR et un membre du comité R concernant la destruction de documents par le SGR</i>	<i>-97-</i>
TITRE III : CONTACTS DU COMITE		-102-
<u>Chapitre 1 :</u>	<i>Journées d'étude</i>	
	<i>15 septembre 1998 : Techniques de protection pour le 21ème siècle</i>	
	<i>2 octobre 1998 : Les droits de l'homme sur Internet</i>	<i>-103-</i>
	Professeur Dumortier	-103-
	Monsieur P. Van Eecke	-104-
<u>Chapitre 2 :</u>	<i>Rapport de la participation d'un membre du comité R au séminaire "l'analyste d'images, au coeur du système d'observation spatiale" organisé à madrid les 15 et 16 octobre 1998</i>	<i>-107-</i>
<u>Chapitre 3 :</u>	<i>Compte-rendu du colloque "Secret d'état ou transparence ?" 20 janvier 1999</i>	<i>-109-</i>
	Monsieur J-P Poncelet, vice-premier ministre et ministre de la Défense nationale	-110-
	Amiral Lacoste	
	<i>"Justifications et légitimité du secret d'Etat"</i>	<i>-110-</i>

Monsieur David Bickford "Balanced secrecy in the new information age"	-111-
Monsieur Ton Beers "Un modèle d'analyse juridique"	-112-
Monsieur Rémi Hyppia "Peut-on protéger les secrets d'Etat tout en faisant preuve de transparence ?"	-112-
Monsieur Jan Van Erps - député "Présentation du projet de loi relatif à la classification et aux habilitations de sécurité"	-112-
Madame Anne Krywin "Le secret d'Etat et les droits de l'homme"	-113-
Monsieur Walter De Bock	-113-
Monsieur Yves Pouillet "Secret d'Etat et vie privée : ou comment concilier l'inconciliable"	-114-
Monsieur Robert Andersen "La mise en balance des intérêts en cause dans l'appréciation des motifs d'exception à la publicité de l'administration"	-115-
<u>Chapitre 4 :</u> Rapport succinct relatif à la participation du comité R à la conférence des organismes de surveillance des activités de renseignement, s'étant tenue à Ottawa les 28 et 29 juin 1999 sur le thème : "examen et surveillance dans le nouveau millénaire : les défis d'un monde multipolaire."	-116-
<u>Chapitre 5 :</u> Rapport succinct relatif à la participation du comité "R" aux journées d'échange de vues organisées les 6 et 7 septembre 1999 à Bucarest à l'initiative des commissions parlementaires roumaines de suivi des services de renseignements	-118-
TITRE IV : HISTORIQUE DU COMITE R	-120-
Composition et fonctionnement du comité permanent R	-121-
Le greffier du comité permanent R	-122-
Le service d'enquêtes du comité permanent R	-122-

Le personnel administratif du comité R	-123-
Les activités du comité permanent R	-123-
Les moyens financiers du comité permanent R	-124-
Activites conjointes avec le comité permanent P	-124-

*

*

*

TITRE I : ACTIVITES DU COMITE PERMANENT R

APERCU ET PERSPECTIVES

ACTIVITES DU COMITE PERMANENT R APERCU ET PERSPECTIVES

Le Comité permanent de contrôle des services de renseignements, couramment dénommé "le Comité permanent R" a été créé par la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements (M.B. 26 juillet 1991).

La création du Comité permanent R faisait suite aux recommandations de deux commissions d'enquêtes parlementaires qui ont notamment conclu à la nécessité d'une loi organique sur les services de renseignement, ainsi qu'à celle d'un contrôle externe sur ces services.

La double mission légale du Comité permanent R était définie à l'époque de la façon suivante : garantir la protection des droits que la Constitution et la loi confèrent aux personnes et assurer la coordination et l'efficacité des services de renseignements ⁽¹⁾.

Le Comité permanent R a débuté ses activités le 26 mai 1993 de manière paradoxale, c'est-à-dire en l'absence de toute loi réglementant les missions et les méthodes des services de renseignements (la Sûreté de l'Etat et le Service général du renseignement et de la sécurité des Forces armées).

Le principe sur lequel se fondait l'action de ces services tenait en cette formule lapidaire : "Tout ce qui n'est pas interdit au citoyen est permis aux services de renseignements".

De sorte à pouvoir, dans ce contexte, exercer au mieux son rôle de contrôleur, le Comité permanent R a, dès le début, pris de nombreux contacts avec des autorités étrangères et a procédé à plusieurs études de droit comparé, notamment :

S "Etude comparative de certaines législations étrangères sur les services de renseignements" (rapport annuel 1995 - p. 4 à 35);

S "L'Allemagne" (rapport annuel 1996 - p. 2 à 18);

⁽¹⁾ L'article 1^{er} de la loi du 18 juillet 1991 a été modifié par la loi du 1^{er} avril 1999. La mission du Comité R est redéfinie comme étant le contrôle de la protection des droits que la Constitution et la loi confèrent aux personnes, et celui de la coordination et de l'efficacité des services de renseignements et de sécurité (M.B. 03/04/1999 - p.11.161)

- S "Etude de la législation néerlandaise sur les services de renseignement et de sécurité" (rapport annuel 1997 - p. 2 à 38);
- S "Etude de la législation du Royaume-Uni relative aux services de renseignements et de sécurité" (rapport annuel 1998 - p. 2 à 42).

Le but poursuivi était de dégager les différents principes susceptibles de fonder un texte légal, en examinant les lois existantes ainsi que les modalités de contrôle appliquées aux services de renseignements d'autres pays.

En se basant sur ces études et les premières enquêtes de contrôle, le Comité permanent R a dégagé, au fur et à mesure, ce qui lui a paru constituer les principes de base nécessaires au fonctionnement efficace des services de renseignements dans un état démocratique, à savoir :

1. un cadre légal comprenant une définition claire des missions de ces services dans un contexte national et international;
2. l'octroi d'un budget adapté aux missions qui leur ont été assignées;
3. la mise à leur disposition d'un personnel suffisant, qualifié et bénéficiant d'un statut garanti;
4. la mise à leur disposition de moyens technologiques suffisants et adaptés à leurs missions;
5. la coordination des activités des services de renseignement et la collaboration effective entre ces services et les services de police;
6. une définition raisonnable et adaptée du secret (secret professionnel, secret des sources, secret de l'information dont la violation est sanctionnée de manière appropriée, etc ...);
7. la possibilité de recourir légalement, et de manière contrôlée, à certaines méthodes spéciales de recherche du renseignement (notamment les écoutes téléphoniques et l'interception de télécommunications).

Le 7 janvier 1997, le Comité permanent R fut d'ailleurs invité à donner, devant les Commissions réunies de la Justice et de la Défense nationale, son avis sur le projet de loi organique des services de renseignement et de sécurité ⁽²⁾.

Le 18 décembre 1998, le Moniteur belge publiait la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

⁽²⁾ Rapport d'activités - 1997 - Titre II - 1ère partie - chapitre 2 - p. 40 et suivantes.

Cette loi définissant l'organisation et les missions de la Sûreté de l'Etat (service civil de renseignement et de sécurité), et du Service général du renseignement et de la sécurité (SGR, service militaire de renseignement et de sécurité), est entrée en vigueur le 1^{er} février 1999.

Le législateur impose à ces services de veiller dans l'exercice de leurs missions au respect et de contribuer à la protection des droits et libertés individuels ⁽³⁾. Ils ne peuvent utiliser des moyens de contrainte que dans les conditions prévues par la loi ⁽⁴⁾.

Ces principes fondamentaux étant posés, la loi organique régit ensuite le recueil et la communication des données, la coopération entre les services, ainsi que la conservation et la destruction des données à caractère personnel.

Des dispositions particulières sont également édictées en ce qui concerne l'exercice des missions de protection des personnes confiées à la Sûreté de l'Etat.

Enfin, le chapitre IV de la loi traite du "secret".

Il convient de souligner d'emblée que toutes ces dispositions normatives sont de nature à permettre au Comité permanent R de donner aujourd'hui, la pleine mesure de sa mission de contrôle telle qu'elle a été redéfinie par la loi du 1^{er} avril 1999 modifiant la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement.

Le législateur énumère et définit les missions des services de renseignement. Parmi les missions reprises dans le cadre de la loi organique se retrouvent bien sûr celles qui, classiquement, étaient déjà exécutées par ces services.

En outre, leur champ d'application a été étendu en ce qui concerne la Sûreté de l'Etat à de nouveaux objectifs, tels "la protection du potentiel scientifique ou économique défini par le Comité Ministériel, ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Comité Ministériel" ⁽⁵⁾.

Pour réaliser ces objectifs, le Comité permanent R a préconisé en 1998 la création d'un organe de concertation entre les ministres concernés et les entreprises détentrices d'un potentiel scientifique, économique ou présentant un intérêt vital pour la Belgique.

⁽³⁾ Loi du 30 novembre 1998 - art. 2 - 2^{ème} alinéa (M.B. 18 décembre 1998).

⁽⁴⁾ Loi du 30 novembre 1998 - art. 12 (M.B. 18 décembre 1998) .

⁽⁵⁾ Loi organique du 30 novembre 1998 - art. 7 1^o (M.B. 18 décembre 1998)

Cet organe devrait pouvoir servir de lieu d'échange d'information entre les entreprises, les universités et les services de renseignement. La Sûreté de l'Etat devrait pouvoir y sensibiliser les milieux académiques, scientifiques et économiques aux menaces de toute provenance ⁽⁶⁾.

En ce qui concerne le SGR, outre les missions classiques liées à la défense nationale, ce service peut se voir confier d'autres missions lorsqu' est en jeu tout autre intérêt fondamental du pays défini par le Roi sur proposition du Comité Ministériel .

Il faut souligner que pour l'accomplissement de ses missions le SGR est autorisé à procéder à des fins militaires à la captation, l'écoute, la prise de connaissance ou l'enregistrement de radiocommunications militaires émises à l'étranger ⁽⁷⁾.

Ce dernier sujet a plus d'une fois retenu l'attention du Comité permanent R. C'est ainsi qu'en 1996 il a consacré un chapitre de son rapport d'activités à une étude de la législation sur les écoutes. En 1997, il a enquêté, à la demande du Parlement, sur les interceptions de télécommunications par le SGR. Le Comité permanent R n' avait alors pu que conclure que ce type d'activité était indispensable.

Depuis 1994, le Comité permanent R a constaté à plusieurs reprises que la collecte, par les services de renseignement, de données à caractère personnel contenues dans les fichiers de différents services publics, s'effectuait de manière informelle et dépendait donc uniquement de contacts individuels et du bon vouloir du fonctionnaire concerné .

La loi organique du 30 novembre 1998 contient une sous-section consacrée au recueil de ces données et décrivant la procédure de communication par les autorités judiciaires, les fonctionnaires et les agents de services publics des informations utiles aux services de renseignement .

Dans le même ordre d'idée, il convient de souligner que deux arrêtés royaux du 8 juillet 1999, publiés au Moniteur belge du 7 août 1999 autorisent le SGR à avoir accès respectivement au registre national des personnes physiques et au registre de la population et des étrangers .

Des projets d'arrêtés visant à octroyer le même accès à la Sûreté de l'Etat sont en cours .

⁽⁶⁾ Rapport d'activités - 1998 - p. 70 et suivantes .

⁽⁷⁾ Loi organique du 30 novembre 1998 - art. 44 (M.B. 18 décembre 1998)

Un autre aspect réglé par le législateur concerne la communication des données par les services de renseignement aux autorités et personnes compétentes conformément aux finalités de leurs missions, ainsi qu'aux instances et personnes qui font l'objet d'une menace visée par la loi. Dans certaines limites imposées notamment par le respect de la vie privée, les services de renseignement peuvent également communiquer des informations à la presse.

En 1995 et 1996, le Comité permanent R a constaté des carences dans la coordination et l'échange d'informations entre le SGR et la Sûreté de l'Etat ⁽⁸⁾.

Dans son rapport d'activités de 1997, a été publiée l'enquête sur la coordination des services de renseignement. Il a été constaté à cette occasion que cette coordination s'était améliorée suite à la conclusion d'un protocole d'accord signé le 20 février 1997 entre la Sûreté de l'Etat et le SGR .

Dans le domaine de la collaboration avec les autorités judiciaires et les services de police, un accord a été signé entre la Sûreté de l'Etat et le Collège des Procureurs Généraux le 15 décembre 1997.

La nouvelle loi organique consacre ces formes de collaboration en édictant que les services de renseignement et de sécurité, les services de police, les autorités administratives et judiciaires veillent à assurer entre eux une coopération mutuelle aussi efficace que possible.

En ce qui concerne la conservation et la destruction des données à caractère personnel par les services de renseignement, le Comité permanent R s'était penché sur ce problème dès 1995 ⁽⁹⁾.

Tenant compte des 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, des critères objectifs en la matière ont été établis après concertation entre les deux services de renseignement et le Comité permanent R.

La loi du 30 novembre 1998 dispose à présent que les données à caractère personnel traitées par les services de renseignement sont conservées pendant une durée n'excédant pas celle nécessaire à la finalité de leurs missions, à l'exception de celles présentant un caractère historique reconnu par les archives de l'Etat. Un arrêté royal déterminera le délai à respecter .

⁽⁸⁾ Rapport d'activités 1995 - pp. 148 et 149
Rapport d'activités 1996 - p. 120 et suivantes

⁽⁹⁾ Rapport d'activités 1996 - p. 97 et suivantes

Depuis des années, une section de la Sûreté de l'Etat est chargée de la protection rapprochée de certaines personnalités étrangères présentes en Belgique. En 1996, le Comité permanent R a enquêté sur le fonctionnement de cette section et a formulé des recommandations visant à octroyer aux agents de protection des compétences de police administrative ⁽¹⁰⁾.

Une section importante de la loi de 1998 est consacrée à cette problématique et donne aux fonctionnaires de larges compétences pour accomplir leurs missions . Les articles relatifs à la protection des personnes s'inspirent de la loi du 5 août 1992 sur la fonction de police, partant du principe que les compétences d'un officier de sécurité ne peuvent en tout cas jamais être plus étendues que celles d'un agent de la force publique .

La loi organique des Services de renseignement et de sécurité reconnaît l'existence d'une obligation de secret professionnel étendu à toute personne concernée par l'application de ses dispositions . Dans cet ordre d'idée, elle contient également des mesures organisant des recours contre des saisies judiciaires ou celles opérées dans le cadre d'une enquête parlementaire, lorsque ces saisies de données ou matériels classifiés sont de nature à constituer une menace pour l'exercice des missions des services de renseignement ou qu'elles présentent un danger pour une personne physique .

En 1995, le Comité permanent R a réalisé une enquête sur la problématique des certificats de sécurité. A la suite de cette enquête , il avait recommandé l'adoption d'une loi claire en la matière répondant aux exigences de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ainsi qu'à celles de l'article 22 de la constitution . Le Comité prônait également l'instauration d'un organe de recours en cas de refus ou de retrait d'un certificat de sécurité ⁽¹¹⁾.

Les 17 février et 20 avril 1998 , le Comité permanent R a été entendu par la Commission de la Défense nationale sur les projets de lois concernant les habilitations de sécurité et la création d'un organe de recours en cette matière ⁽¹²⁾.

A cette occasion, il avait recommandé l'adoption d'une législation globale relative aux documents, renseignements et matériels classifiés , c'est-à-dire ceux que l'autorité peut ou doit garder secret pour des raisons de sécurité et/ ou de protection de la vie privé.

Suite à son rapport d'activités de 1998, le Comité permanent R a également rédigé une étude intitulée : “ *Les devoirs de secret auxquels sont tenus les membres des services de renseignement* .”

⁽¹⁰⁾ Rapport d'activités 1996 , p. 68 et suivantes .

⁽¹¹⁾ Rapport d'activités 1995, p. 112 et suivantes.

⁽¹²⁾ Rapport d'activités 1998, p. 44 et suivantes .

Le 20 janvier 1999, le Comité a organisé en collaboration avec le Centre d'Etudes de Défense de l'Institut Royal Supérieur de Défense (IRSD), un colloque sur le thème "*Secret d'Etat ou Transparence*".

L'objectif de cette manifestation était double : stimuler la réflexion sur la problématique du "secret officiel" et sensibiliser les mondes politique, judiciaire, académique, militaire et des services publics sur la nécessité de légiférer en cette matière dans un environnement international en mutation .

Cette manifestation a réuni des spécialistes belges, européens et canadiens et a attiré plus de 250 participants .

Le Moniteur belge du 7 mai 1999 a publié deux lois du 11 décembre 1998, l'une "relative à la classification et aux habilitations de sécurité", l'autre " portant création d'un organe de recours en matière d'habilitation de sécurité ".

La première définit ce qu'on entend par classification, ce qui peut en faire l'objet, ainsi que les différents degrés de cette classification .

Pour avoir accès aux documents, aux données et au matériel classifiés, la loi prévoit qu'il faut une habilitation de sécurité qui est déterminée par le degré de classification des informations auxquelles on doit avoir accès pour l'exercice de sa fonction ou de sa mission . Des sanctions pénales prévoyant un emprisonnement allant d'un mois à cinq ans sont édictées pour ceux qui violeraient leur obligation de secret .

La même loi édicte la procédure d'octroi de ces habilitations et définit la notion d'enquête de sécurité. Ces dernières sont confiées aux services de renseignement et de sécurité .

La seconde loi instaure le Comité permanent R comme organe de recours en matière d'habilitation de sécurité.

L'entrée en vigueur de ces deux lois sera déterminée par arrêté royal.

Au cours de la période écoulée, le Comité permanent R a effectué d'autres enquêtes de contrôle.

Certaines de celles-ci revêtent une importance que le Comité tient à souligner. Nombre de sujets restent d'ailleurs d'actualité, comme la protection des systèmes informatiques et de communication. Dans ce cadre, le Comité R avait recommandé dès 1994, qu'un organisme officiel soit chargé de concevoir et d'appliquer une politique globale de sécurité pour l'ensemble des systèmes d'information de la fonction publique.

Le groupe BELINFOSEC, suscité par une initiative du SGR, poursuit cet objectif. Il est composé de représentants des milieux académiques, gouvernementaux, industriels préoccupés par les risques que les systèmes automatisés de traitement de l'information font courir aux libertés individuelles et à la survie des entreprises ⁽¹³⁾.

Aux termes de la loi organique, le SGR est investi d'une mission de protection des systèmes informatiques et de communications militaires ou de ceux que le ministre de la Défense nationale gère. Une extension d'une telle mission, à des intérêts autres que militaires, n'est pas mentionnée explicitement dans la loi. Sans doute peut-on comprendre que ce type de mission rentre dans le cadre de la défense du potentiel scientifique ou économique qui est de la compétence de la Sûreté de l'Etat.

On peut citer dans le même ordre d'idée, l'étude et l'enquête réalisée en 1998 sur la participation des services de renseignement belges, spécialement le SGR, à des programmes satellitaires de renseignement. Dans le contexte international d'aujourd'hui, le Comité permanent R considère les images fournies par les satellites d'observation spatiale comme un moyen essentiel d'aide à la prise de décisions politico-militaires (et non exclusivement militaires) en vue de la prévention des conflits et de la gestion de crises, quelles que soient leurs natures (conflits internationaux, guerres civiles, catastrophes environnementales, etc...). L'observation satellitaire est un moyen de recueil du renseignement complémentaire et indispensable par rapport aux autres méthodes classiques.

L'intérêt du Comité permanent R pour cette question répondait à une préoccupation politique concrétisée e.a. dans la déclaration gouvernementale du 28 juin 1995 exprimant la volonté de notre pays de "contribuer activement à l'élaboration d'une architecture de sécurité européenne en vue de promouvoir la stabilité du continent européen et d'éviter de nouveaux clivages" ⁽¹⁴⁾.

Un des aspects qui préoccupe aussi le Comité permanent R concerne les méthodes utilisées par les services pour la récolte du renseignement.

De toutes les méthodes employées, l'utilisation d'informateur est sans doute celle qui est la plus essentielle, mais qui en même temps est la plus délicate, aussi bien du point de vue de l'efficacité des services que du respect des droits du citoyen.

⁽¹³⁾ voir : Rapport d'activités - 1995 - p. 103 et suivantes
Rapport d'activités - 1996 - p. 57 et suivantes
Rapport d'activités - 1997 - p. 186 et suivantes

⁽¹⁴⁾ Rapport d'activités - 1998 - p. 130 et suivantes

Dans son rapport d'activités de 1997, le Comité a réalisé une enquête pour essayer de cerner les problèmes et surtout de mettre en évidence les risques que pose la nécessité du recours à de telles sources.

L'article 18 de la loi organique prévoit le recours à des sources humaines et à la protection de celles-ci. Néanmoins, des directives devront être élaborées concernant notamment le recrutement, la rémunération, la protection et l'évaluation des informateurs.

Un échange de vues entre le Comité permanent R et les services de renseignement au sujet de cette problématique est toujours en cours en tenant compte des principes de subsidiarité et de proportionnalité à appliquer dans ce domaine⁽¹⁵⁾.

Enfin, un aspect important des missions du Comité permanent R a été d'enquêter sur les plaintes introduites par des particuliers estimant avoir été lésés par l'intervention d'un service de renseignement.

Aucune de ces enquêtes n'a conclu à l'existence d'une atteinte disproportionnée ou injustifiée aux droits et libertés des plaignants.

En conclusion, on peut souligner que différentes lois importantes concernant le monde du renseignement ont été promulguées ces derniers temps.

Ces dispositions devraient non seulement faciliter la tâche des services de renseignement, mais aussi permettre au Comité d'exercer sa mission de contrôle de manière plus ciblée. On peut également considérer que ces deux aspects constitueront également pour le citoyen une protection accrue de ses droits et libertés fondamentales.

La loi organique définit les missions de la Sûreté de l'Etat et du SGR, tout en consacrant la communication obligatoire des renseignements aux instances et personnes compétentes, Ces dispositions posent la question du contrôle de la communication de renseignements utiles aux bénéficiaires. Il est important de souligner que ce contrôle peut être effectué par le Comité R à la demande des ministres compétents. A ce sujet, le Comité permanent R se réfère à la citation suivante de M. David Bickford :

“Information has to be made available to independent oversight bodies to ensure that they effectively oversee the administration and operations of the law enforcement and intelligence agencies and others used in the fight against crime”⁽¹⁶⁾.

⁽¹⁵⁾ Rapport d'activités - 1997 - p. 134 et suivantes.

⁽¹⁶⁾ Citation extraite du texte de Monsieur David Bickford - Colloque du 20 janvier 1999 - *“Secret d'Etat ou transparence ?”*.
M. David Bickford fut conseiller juridique des services secrets du Royaume-Uni de 1987 à 1995.

Les défis lancés aux services de renseignement par les nouvelles missions qui leur sont confiées impliquent la mise en oeuvre de moyens adéquats et suffisants aussi bien dans le domaine du personnel et du matériel mis à leur disposition que dans celui de la formation.

Dans cette optique, le développement de l'exploitation et de l'analyse des sources ouvertes⁽¹⁷⁾ auxquelles ont de plus en plus souvent recours non seulement tous les services de renseignement, mais e.a. également les services de police ou de détection du blanchiment, notamment dans la lutte contre le crime organisé et le terrorisme, mérite une attention particulière.

Ceci nécessitera non seulement une étroite collaboration entre les services pour se partager ces sources, mais également l'acquisition de programmes informatiques adaptés, permettant d'optimiser les analyses.

Enfin, l'arsenal législatif devrait être complété par des mesures permettant aux services de renseignement d'effectuer, sous contrôle, des interceptions de sécurité⁽¹⁸⁾ pour assurer avec efficacité leurs missions tant sur le plan national, que dans le cadre de leur collaboration avec d'autres services de renseignement.

Si les moyens ne devaient pas être à la mesure de l'importance des missions, on prendrait sans doute le risque de voir se développer des multinationales privées du renseignement qui échapperont au contrôle démocratique des Etats. Ce risque est particulièrement à souligner dans la matière de la protection du potentiel économique .

⁽¹⁷⁾ Rapport d'activités - 1996 - p. 230

⁽¹⁸⁾ Voir à ce sujet dans le présent rapport d'activités l'enquête concernant la manière dont les services belges de renseignement réagissent face à l'éventualité d'un système américain "Echelon" d'interception des communications téléphoniques et fax en Belgique.

TITRE II : NOS SERVICES DE RENSEIGNEMENT

LES ENQUETES

A. A LA REQUETE DU PARLEMENT OU DES MINISTRES

CHAPITRE 1 : RAPPORT DE L'ENQUÊTE SUR LA COLLECTE DE DONNÉES PAR LES SERVICES DE RENSEIGNEMENTS À PROPOS DES PARLEMENTAIRES

1. INTRODUCTION

Suite à la lecture du rapport d'enquête sur *“la manière dont les services de renseignements font la distinction entre les activités de parlementaires en tant que pacifistes écologistes et en tant que parlementaires”* ⁽¹⁾, les Commissions spéciales chargées de l'accompagnement parlementaire des Comités permanents de contrôle des services de police et de renseignements ont souhaité que le Comité R examine plus généralement la collecte de données par les services de renseignement à propos des parlementaires.

2. PROCEDURE

Les présidents des Commissions spéciales chargées de l'accompagnement parlementaire des Comités permanents de contrôle des services de police et de renseignements ont adressé la demande d'enquête au Comité R le 17 juillet 1998.

Ces Commissions ont aussi demandé que le Comité R fasse annuellement rapport sur ce sujet.

Le Comité R a décidé d'ouvrir cette enquête le 30 juillet 1998. Deux de ses membres ont été chargés d'en suivre le déroulement et d'en faire rapport.

Le Comité R a aussi décidé de limiter l'enquête aux membres du Parlement fédéral de la législature en cours et de mener celle-ci de la même manière que celle relative aux parlementaires écologistes.

Le Comité R a adressé une apostille en ce sens au chef du Service d'enquêtes le 5 août 1998.

Le Comité R lui a aussi demandé de vérifier si les partis politiques faisaient l'objet d'un quelconque suivi de la part des services de renseignement.

(1) Comité R - rapport d'activités - 1998 - p. 60 à 68

Le 10 août 1998, le greffier du Comité R a notifié l'ouverture de l'enquête à :

- Monsieur Frank Swaelen, Président du Sénat et Président de la Commission spéciale du Sénat chargée de l'accompagnement parlementaire des Comités permanents de contrôle des services de police et de renseignements ;
- Monsieur Raymond Langendries, Président de la Chambre des Représentants ;
- Monsieur Robert Delathouwer, Président de la Commission spéciale de la Chambre des Représentants chargée de l'accompagnement parlementaire des Comités permanents de contrôle des services de police et de renseignements.

Le 19 août 1998, conformément à l'article 43, alinéa 1 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, le chef du Service d'enquêtes R a notifié l'ouverture de l'enquête aux ministres compétents.

Le 20 août 1998, le chef du Service d'enquêtes a demandé aux présidents de la Chambre des Représentants et du Sénat de lui faire parvenir une liste complète des membres de ces assemblées avec la date de naissance de chacun des parlementaires, afin de pouvoir vérifier l'existence éventuelle d'un dossier au nom de chacun d'eux.

La liste des membres de la Chambre des Représentants a été reçue le 24 août 1998, tandis que celle des membres du Sénat a été reçue le 25 août 1998.

Le Général W. Simons, Chef du SGR et Monsieur B. Van Lijsebeth, Administrateur général de la Sûreté de l'Etat, ont été prévenus du démarrage de l'enquête le 7 octobre 1998.

Le Service d'enquêtes du Comité R a entamé ses premiers devoirs d'enquête le 27 octobre 1998.

Le 12 novembre 1998, le chef du Service d'enquêtes a demandé aux présidents de la Chambre des Représentants et du Sénat de lui faire connaître la date de la première investiture de chacun des parlementaires, ceci afin d'examiner s'il existait un lien entre la constitution d'un dossier par les services de renseignement et l'exercice d'un mandat parlementaire.

Le rapport final du Service d'enquêtes a été transmis au Comité R le 23 décembre 1998.

Le Comité R a approuvé le présent rapport le 16 juin 1999.

3. L'INTÉRÊT PARLEMENTAIRE

L'intérêt du Parlement pour cette enquête est démontré à suffisance par le fait même qu'elle a été ouverte à l'initiative des Commissions spéciales du Sénat et de la Chambre des Représentants chargées de l'accompagnement parlementaire des Comités permanents de contrôle des services de police et de renseignements.

4. LES DOSSIERS DE LA SÛRETÉ DE L'ETAT

Afin de bien comprendre la démarche suivie par le Service d'enquêtes du Comité R pour mener cette enquête, il est nécessaire d'exposer ici la manière dont les dossiers individuels de la Sûreté de l'Etat sont constitués et traités.

4.1. La constitution des dossiers en général

Plusieurs notes de service récentes contiennent les directives de la Sûreté de l'Etat qui indiquent les cas dans lesquels des rapports sont rédigés par ce service et ceux dans lesquels des dossiers individuels sont constitués.

Certaines de ces notes sont antérieures à la mise en vigueur de la loi du 30 novembre 1998, organique des Services de renseignement et de sécurité.

La Sûreté de l'Etat constitue des dossiers individuels sur des personnes :

- qui ont fait l'objet d'une enquête de sécurité d'une part,
- qui ont fait l'objet d'un rapport en relation avec l'un des sujets repris dans la liste des sujets de ce service d'autre part.

En rapport avec les sujets généraux, des dossiers individuels sont constitués pour les personnes qui déploient des activités qui peuvent représenter une atteinte aux fondements de l'Etat de droit.

La liste des sujets de la Sûreté de l'Etat est une liste non exhaustive d'organisations, de groupes et d'activités qui relèvent de l'application de la définition légale de la sphère d'intérêt de ce service, c'est-à-dire qui représentent pour la Belgique une menace réelle ou potentielle au sens de la loi du 30 novembre 1998, organique des Services de renseignement et de sécurité (*selon les articles 7 et 8 : l'espionnage, le terrorisme, l'extrémisme idéologique, la prolifération, les sectes nuisibles, les organisations criminelles, l'ingérence*).

Cette liste a toutefois évolué au cours des années avant de s'en tenir aux critères des menaces définis dans la loi du 30 novembre 1998.

Tous les dossiers font actuellement l'objet d'une procédure de sélection pour être : soit conservés, soit archivés, soit détruits.

Les dossiers à détruire et à transférer aux Archives générales du Royaume sont conservés dans un local à part en attendant qu'ils soient effectivement traités de la sorte.

La destruction effective des dossiers n'aura lieu qu'à l'issue du processus de classement qui aura probablement lieu dans deux ans.

L'intention est de soumettre le résultat final de ce classement à la Commission de protection de la vie privée, au Comité R et aux Archives du Royaume.

En attendant, les références de ces dossiers ont été effacées du fichier informatique central pour être conservées dans un fichier séparé.

4.2. L'examen des dossiers des parlementaires

Le Service d'enquêtes du Comité R a établi une fiche pour chacun des 71 sénateurs (à l'exception des membres de la famille royale) et 150 députés.

Les fiches des parlementaires pour lesquels le Service d'enquêtes a constaté l'existence d'un dossier individuel à la Sûreté de l'Etat ont ainsi été complétées.

Les fiches des parlementaires pour lesquels le Service d'enquêtes n'a pas constaté l'existence d'un dossier individuel à la Sûreté de l'Etat ont reçu la mention "NIHIL".

Parmi les 221 parlementaires (députés et sénateurs, à l'exception des membres de la famille royale), un certain nombre fait l'objet d'un dossier individuel auprès de la Sûreté de l'Etat.

Tous ces dossiers ont été ouverts bien avant l'entrée en vigueur de la loi du 30 novembre 1998, organique des services de renseignement et de sécurité.

La plupart ont aussi été ouverts avant l'élection de leur titulaire au Parlement. Ils reflètent un intérêt pour des mouvements et tendances qui, à l'époque, étaient considérés comme étant à suivre par la Sûreté de l'Etat.

La Sûreté de l'Etat n'a procédé à aucune enquête de sécurité sur aucun des parlementaires de l'actuelle législature.

4.3. Les demandes de consultation de dossiers individuels introduites par des parlementaires

Au cours de l'année 1995, des parlementaires/membres des groupes politiques Ecolo/ Agalev et Vlaams Blok ont demandé à pouvoir consulter leurs dossiers individuels tenus par la Sûreté de l'Etat.

Toutes ces demandes, fondées sur la loi du 11 avril 1994 relative à la publicité de l'administration, ont été rejetées sur base des exceptions relatives à la sûreté nationale et à la vie privée prévues par l'article 6 de la loi précitée.

Les refus firent également référence à la loi du 8 décembre 1982 relative à la protection de la vie privée et aux compétences exclusives de la Commission de la protection de la vie privée au sujet de l'exercice du droit d'accès et de rectification des données à caractère personnel ⁽²⁾.

⁽²⁾ Comité R - rapport d'activités - 1997 : p. 53 à 73.

Néanmoins, le ministre de la Justice précisa à l'intention des requérants que :

- la Sûreté de l'Etat n'établissait jamais de dossiers individuels en raison d'activités parlementaires et n'effectuait pas d'enquêtes concernant des actes accomplis dans l'exercice d'un mandat parlementaire;
- les dossiers constitués au fil des années pouvaient continuer à exister, même si la matière, autrement dit le sujet à la base du dossier, ne figurait plus sur la liste actualisée.

4.4. Le jugement du Tribunal de Première Instance de Bruxelles du 5 décembre 1997

Le 5 décembre 1997, le Tribunal de Première Instance de Bruxelles a rendu un jugement à l'encontre de la Sûreté de l'Etat et ce, à la requête de trois parlementaires du Vlaams Blok : un membre du Parlement flamand, un membre de la Chambre des Représentants et un membre du Sénat.

L'action visait à faire dire pour droit que l'Etat belge se rendait coupable d'une atteinte à la vie privée des requérants en ce que la Sûreté de l'Etat et la gendarmerie collectaient des données personnelles sur leurs personnes.

La demande se fondait sur l'article 8 de la convention européenne des droits de l'homme. La demande a été jugée partiellement fondée.

Constatant en effet que la Sûreté de l'Etat n'avait pas encore reçu à cette époque de mission légale lui permettant de s'immiscer dans la vie privée des citoyens à des fins de sécurité, le tribunal a fait défense à ce service d'encore collecter des données personnelles sur les trois requérants.

L'un des requérants entendait en outre introduire sa demande au nom de tous les membres de son parti. Cette demande a été jugée irrecevable par le tribunal.

Ce jugement n'a pas encore acquis force de chose jugée car l'Etat a interjeté appel.

L'Administrateur général de la Sûreté de l'Etat estime quant à lui que ce jugement est dépassé par le fait même de l'entrée en vigueur de la loi organique sur les services de renseignement et de sécurité.

4.5. Destination des dossiers après examen et tri

Il apparaît que seuls les dossiers de parlementaires qui ont encore des activités en rapport avec l'un des sujets actuels de la Sûreté de l'Etat ont reçu la mention "TE BEWAREN - À CONSERVER".

5. LES DOSSIERS DU SGR

5.1. La constitution de dossiers sur les parlementaires

Suite au rapport de l'enquête menée par le Comité R sur *“la manière dont les services de renseignements font la distinction entre les activités de parlementaires en tant que pacifistes écologistes et en tant que parlementaires”*, le ministre de la Défense nationale a donné des instructions extrêmement strictes au SGR en ce qui concerne la collecte d'informations ne provenant pas de sources ouvertes concernant des parlementaires.

Le SGR a donné suite à cette instruction ministérielle.

Le SGR a étudié l'épuration systématique de tous ces dossiers et passera à l'exécution de ce travail dès qu'il disposera des moyens qualifiés nécessaires.

Cependant, suite au rapport de l'enquête menée par le Comité R, le SGR a retiré des dossiers des parlementaires concernés toute trace éventuelle d'informations qui ne proviennent pas de sources ouvertes.

Cette opération a été exécutée en juillet 1998 suite à la demande du ministre.

La méthode d'examen des dossiers de parlementaires au SGR a été la même qu'à la Sûreté de l'Etat.

Un certain nombre des 221 parlementaires (députés et sénateurs, à l'exception des membres de la famille royale), fait l'objet d'un dossier individuel auprès du SGR.

Le Service d'enquêtes du Comité R a de nouveau constaté que les dossiers du SGR ne contenaient aucun inventaire des pièces qui les constituent et que celles-ci n'étaient pas cotées. Cette lacune constitue un obstacle à la fiabilité du contrôle.

Près de la moitié de ces dossiers ont été ouverts à l'occasion d'enquêtes de sécurité effectuées à une époque où les intéressés étaient revêtus de fonctions militaires ou bien exerçaient des activités civiles en rapport avec la Défense nationale.

Certains de ces dossiers ont été ouverts en raison de demandes d'autorisation de prises de vues aériennes (en application de l'arrêté royal du 21 février 1939 et de l'arrêté ministériel du 28 février 1940 réglementant les prises de vues aériennes au-dessus du territoire national).

Enfin, l'autre moitié des dossiers contient des renseignements au sujet d'activités politiques au sein de mouvements extrémistes ou de prises de position antimilitaristes des intéressés. Certains de ces dossiers ont été ouverts après l'élection des intéressés à une fonction parlementaire, mais ils ne se rapportent pas à leurs activités parlementaires proprement dites.

6. CONCLUSIONS GÉNÉRALES

Le Comité R confirme que ni la Sûreté de l'Etat, ni le SGR n'effectuent d'enquêtes concernant des actes accomplis dans l'exercice proprement dit d'un mandat parlementaire.

7. RECOMMANDATIONS

Le Comité R recommande :

- à la Sûreté de l'Etat de poursuivre son opération de tri de ses dossiers.

- au SGR :

- * d'entamer sans tarder une opération de tri de ses dossiers de manière à ne conserver que ceux qui présentent un rapport avec ses missions légales
- * une nouvelle fois, de coter les pièces qui constituent un dossier et d'en faire l'inventaire dans chaque dossier.

CHAPITRE 2 : RAPPORT RELATIF A UNE DEMANDE D'ENQUETE EMANANT DU DEPUTE OLIVIER DELEUZE, QUANT A L'INTERCEPTION SUPPOSEE PAR LA SURETE DE L'ETAT DE COURRIER DANS LE CADRE D'UNE ENQUETE JUDICIAIRE

1. PROCÉDURE

Les présidents des Commissions spéciales chargées de l'accompagnement parlementaire des Comités permanents de contrôle des Services de police et de renseignements ont adressé le 17 juillet 1998 au Comité R une lettre du député Olivier Deleuze dans laquelle celui-ci demandait l'ouverture d'une enquête relative à une intervention de la Sûreté de l'Etat, qui aurait intercepté du courrier. A l'occasion de cette demande il sollicitait, en outre, la saisine du Comité R aux fins d'indaguer sur les activités de la Sûreté de l'Etat en rapport avec des dossiers à l'instruction, particulièrement sur le point relatif à l'ouverture du courrier.

Les Commissions ont souhaité que le Comité R examine le rôle de la Sûreté de l'Etat dans le dossier concerné.

Lors de sa réunion du 30 juillet 1998, le Comité R décida d'ouvrir une enquête sur le rôle de la Sûreté de l'Etat dans une éventuelle interception de courrier dans le cadre d'une instruction judiciaire.

Deux de ses membres ont été chargés d'en suivre le déroulement et d'en faire rapport .

Le 10 août 1998, le greffier du Comité R notifiait l'ouverture de l'enquête à :

- Monsieur Frank Swaelen, Président du Sénat et Président de la Commission spéciale du Sénat chargée de l'accompagnement parlementaire des comités permanents de contrôle des services de police et de renseignements;
- Monsieur Raymond Langendries, Président de la Chambre des représentants ;
- Monsieur Robert Delathouwer, Président de la Commission spéciale de la Chambre des représentants chargée de l'accompagnement parlementaire des comités permanents de contrôle des services de police et de renseignements.

Par courrier du 19 août 1998, conformément à l'article 43.1° de la loi organique du 18 juillet 1991, le chef du Service d'enquêtes avertissait le Ministre de la Justice de l'ouverture de l'enquête.

Le 17 août 1998 une apostille mentionnant plusieurs devoirs était transmise au chef du Service d'enquêtes.

2. L'INTÉRÊT PARLEMENTAIRE

Celui-ci se manifeste par l'interpellation de Monsieur Olivier Deleuze (Député Ecolo) au Ministre de la Justice sur l'inviolabilité du courrier dans notre pays (n° 1903) - Chambre des représentants - COM 25.05.1998.

3. DÉROULEMENT DE L'ENQUÊTE

3.1. Recherche des procès-verbaux

En annexe à sa lettre, le Député Olivier Deleuze donnait les références de deux procès-verbaux.

Après avoir obtenu l'accord des Procureurs Généraux concernés le Service d'enquêtes a pris connaissance du contenu des dossiers judiciaires.

3.2. Auditions

Le 31 août 1998, la Présidente du Comité R et le Chef du Service d'enquêtes ont entendu Monsieur le Député Olivier Deleuze .

Par la suite, la personne victime des agissements supposés de la Sûreté de l'Etat prit contact avec le Service d'enquêtes et fit l'objet d'une audition le 25 novembre 1998. Le plaignant a précisé qu'il avait été entendu dans le courant de l'année 1997 par la Gendarmerie à propos d'un courrier dont il était le destinataire, mais qui ne lui était jamais parvenu.

Sa plainte était essentiellement fondée sur le fait qu'il soupçonnait la Sûreté de l'Etat d'une interception de ce courrier.

Il se posait dès lors des questions au sujet des agissements de la Sûreté de l'Etat en général et plus particulièrement en ce qui concerne le secret de la correspondance.

3.3. Eléments du dossier du Parquet

Le 15 décembre 1998, le Service d'enquêtes du Comité R en la personne de son chef de service prend connaissance et copie des différents procès-verbaux du dossier de cette information, par ailleurs classée sans suite par le Parquet de Bruxelles.

En résumé, il ressort de ce dossier ce qui suit : à une date qu'elle situe le 16 mars 1997, une employée de la poste éprouve des difficultés à identifier le destinataire d'une lettre. La rédaction du nom n'est pas claire et ne correspond pas au titulaire de la boîte postale.

En effet, le titulaire de celle-ci n'est autre que le plaignant tandis que la missive est adressée à un mouvement politique dont il apparaîtra par la suite que le plaignant fait partie .

Conformément aux règlements en vigueur, l'employée de poste ouvre la missive et se trouve fortement ébranlée par son contenu qui fait, notamment, référence à la vente de cassettes pornographiques à caractère pédophilique. L'employée en avertit son supérieur hiérarchique.

Selon les investigations du Service d'enquêtes ce supérieur avait déjà reçu la visite d'un agent de la Sûreté de l'Etat, lequel s'était toutefois borné à demander l'identification du titulaire de la boîte postale dont question.

Après lecture du contenu de la lettre, le supérieur hiérarchique alertera finalement la gendarmerie le 27 mars 1997.

Suite à ces développements, une information fût menée par le Parquet du Procureur du Roi de Bruxelles . Sur base des informations recueillies, le dossier répressif fût classé "sans suite".

3.4 Les dossiers à la Sûreté de l'Etat

Le Service d'enquêtes a pris contact avec l'Administrateur Général de la Sûreté de l'Etat afin de procéder à l'examen des dossiers individuels des personnes citées dans les procès-verbaux, pour autant qu'elles fussent connues de son administration. Le Service d'enquêtes s'est rendu au siège de la Sûreté de l'Etat pour procéder à diverses investigations.

Il en est résulté que le plaignant ainsi que le mouvement politique auquel il appartient, sont connus de la Sûreté de l'Etat.

La Sûreté de l'Etat s'est limitée à identifier le titulaire de cette boîte postale.

Il appert que l'identification, par la Sûreté de l'Etat, du titulaire de la boîte postale relève d'un processus de simple mise à jour dans le cadre de l'exploitation logique des renseignements via les sources ouvertes et non d'une violation des garanties constitutionnelles consacrées par l'article 29 de la Constitution.

Tous ces éléments sont publics et ne résultent nullement d'infractions commises par la Sûreté de l'Etat en matière de protection des libertés fondamentales.

Le contenu du dossier de la Sûreté de l'Etat concernant le plaignant ne permet pas d'établir l'existence d'une quelconque surveillance de son courrier.

4. CONCLUSIONS

Il ressort de l'enquête que la Sûreté de l'Etat n'a pas commis de faits constitutifs de violation du secret de la correspondance consacré par l'article 29 de la Constitution.

CHAPITRE 3 : RAPPORT D'ENQUÊTE SUR LA MANIÈRE DONT LES SERVICES BELGES DE RENSEIGNEMENT RÉAGISSENT FACE À L'ÉVENTUALITÉ D'UN SYSTÈME AMÉRICAIN "ECHELON" D'INTERCEPTION DES COMMUNICATIONS TÉLÉPHONIQUES ET FAX EN BELGIQUE

1. INTRODUCTION

Une étude de septembre 1998, intitulée *"Une évaluation des techniques de contrôle politique"* rédigée par la Fondation Omega de Manchester et présentée au groupe STOA (Scientific and Technological Assessment) du Parlement Européen a éveillé un grand intérêt dans la presse de toute l'Union européenne.

Cette étude révélait l'existence d'un réseau *"Echelon"*, qui aurait été mis en place par les Etats-Unis et par la Grande Bretagne, en vue d'intercepter toutes les communications électroniques, téléphoniques et par fax en Europe.

La diffusion de ce rapport par les médias a éveillé l'attention de certains gouvernements, français notamment, ainsi que de certains parlementaires belges.

2. PROCÉDURE

Par courrier du 10 novembre 1998, Monsieur le Député Delathouwer, Président de la Commission spéciale chargée de l'accompagnement parlementaire des Comités "P" et "R" a adressé au Comité R une demande d'enquête rédigée en ces termes :

"comment les services belges de renseignements réagissent-ils face à l'éventualité d'un système américain "Echelon" d'interception des communications téléphoniques et fax en Belgique ?"

Nos services cherchent-ils à en établir l'existence et, le cas échéant, à protéger les entreprises et les citoyens belges contre ces interceptions ?

Le Comité R a décidé d'ouvrir cette enquête le 12 novembre 1998. Deux de ses membres ont été chargés de la suivre et de faire régulièrement rapport de son déroulement.

Le 18 novembre 1998, les Présidents du Sénat et de la Chambre, ont été avertis de l'ouverture de cette enquête.

Par lettres du 27 novembre 1998, le Service d'enquêtes a averti les Ministres de la Justice et de la Défense Nationale de l'ouverture de l'enquête.

Le 30 novembre 1998, le Comité R a transmis au chef du Service d'enquêtes une apostille détaillée, une note de synthèse ainsi que la documentation qu'il avait déjà rassemblée sur ce sujet.

Le 2 février 1999, un courrier a été adressé à Monsieur l'Administrateur général de la Sûreté de l'Etat afin d'obtenir les coordonnées de la personne qui serait l'interlocuteur de référence en cette matière. Le 24 février un courrier similaire fut adressé au Général-Major Simons, en sa qualité de responsable du SGR.

Le Service d'enquêtes a déposé son rapport le 22 mars 1999; celui-ci a été discuté par le Comité R le 7 juin 1999.

Au cours des mois de juin et juillet 1999, le Comité R a complété son information.

Le présent rapport a été approuvé par le Comité R le 5 août 1999.

3. L'INTÉRÊT PARLEMENTAIRE

Remarque préliminaire : la présente enquête est le résultat d'une initiative parlementaire fédérale. L'intérêt parlementaire vis-à-vis de cette problématique est dès lors évident. Le Comité R a en outre relevé les quelques questions et interpellations suivantes :

3.1. Au niveau fédéral

S Le 16 février 1998, question de Monsieur le Député Robert Delathouwer (SP) au Ministre de la Justice, Monsieur Stefaan De Clerck, au sujet du réseau "Echelon" ou le système de captage de toutes communications téléphoniques, fax et e-mail en Europe (nr.740 - Chambre des Représentants -COM 16.02.1998) .

Réponse du Ministre de la Justice :

"La Sûreté de l'Etat ne dispose d'aucune indication quant à l'existence de ce réseau..... La Sûreté de l'Etat ne se prête pas à des pratiques d'espionnage, ne reçoit pas d'informations illégalement recueillies et ne les utiliserait pas .

Le 28 novembre 1997, le comité ministériel chargé des renseignements et de la sûreté a ordonné une enquête sur les menaces d'espionnage économique pour les secteurs socio-économiques. Le service de renseignements disposera des moyens nécessaires pour mener à bien cette nouvelle mission .

Cette question s'inscrit dans un cadre plus large et concerne notamment les législations nationales et européennes en matière de télécommunications . Celles-ci devront prévoir les protections nécessaires. Je songe en l'occurrence à des inscriptions et à des verrouillages."

- Le 8 octobre 1998, interpellations jointes par Messieurs les Députés Robert Delathouwer (SP) et Olivier Deleuze (Ecolo) au Ministre des Affaires Etrangères, Monsieur Erik Derijcke sur le “système Echelon d’interception des télécommunications en Europe” (nE 2022) et “l’interception de télécommunications en Europe par le système Echelon” (nE 2056), dans le cadre de l’étude du Parlement Européen du 14 septembre 1998 au sujet de “l’évaluation des techniques de contrôle politique”. (Chambre des Représentants - COM 08-10-1998).

Réponse du Ministre :

“

La commission européenne a toujours répondu qu’elle ne disposait pas de preuves et qu’elle n’avait pas enregistré la moindre plainte .

C’est le rapport d’un bureau d’études indépendant britannique qui est à la base de ces rumeurs d’interception . Ce document n’a toutefois pas encore été rendu public et n’a pas encore été discuté au Parlement européen. J’ai demandé un exemplaire de ce rapport à notre représentant auprès de l’UE. Je l’ai transmis au ministre de la Justice. Si cette histoire est confirmée, c’est à la Justice d’intervenir . La Justice m’a fait savoir que l’enquête est toujours en cours .

Il existerait une interaction au niveau des administrations nationales.

.....

S’il s’avère que certains faits se sont réellement produits, il conviendra de réfléchir aux réactions diplomatiques qu’ils appellent . Dans ce cas, j’estime que les pays de l’Union européenne devraient réagir conjointement . La question est de savoir dans quelle mesure les autres pays ont profité de ce système . L’Union européenne se penche actuellement sur le cryptage ainsi que sur son impact sur la législation en matière de télécommunications .

.....

La nouvelle loi du 19 décembre 1997 concernant les télécommunications libéralisait le cryptage en Belgique .

.....”

- Le 19 octobre 1998, question orale posée par Monsieur le Député Yves Leterme (C.V.P.) au Ministre de la Justice, Monsieur Tony Van Parijs, sur la transposition de la directive 97/66/CE du Parlement Européen et du Conseil du 15 décembre 1977 relative au traitement des données personnelles et à la protection de la vie privée dans le secteur des télécommunications (nE1469 - Chambre des Représentants - COM 19.10.98) .
- Le 26 octobre 1998, interpellation par Monsieur le Député Olivier Deleuze (Ecolo) au Ministre de la Justice, Monsieur Tony Van Parijs, relativement à la publication, par le Parlement Européen, en date du 14 septembre 1998, d’une étude relative à l’évaluation des techniques de contrôle politique parmi lesquelles le système “Echelon” (nE2067- Chambre des Représentants - COM 26-10-1998) .

Réponse du Ministre :

“

....le document a été transmis aux services compétents , dont l'administration de la Sûreté de l'Etat et la Commission pour la protection de la vie privée, avec la demande de le soumettre à une lecture critique et de procéder éventuellement à une enquête plus poussée.

A l'heure actuelle, l'enquête est toujours en cours

S'il devait s'avérer, notamment à la lumière de la législation belge , que les résultats de l'enquête sont effectivement préoccupants en ce qui concerne la protection de la vie privée, le ministre des Affaires étrangères en sera immédiatement informé, en particulier dans le but d'examiner quelles initiatives s'imposent dans le cadre de l'Union européenne .”

- Le 12 janvier 1999, question orale posée par Monsieur le Député Olivier Deleuze (Ecolo) au Ministre de la Justice, Monsieur Tony Van Parijs, afin de savoir où en sont les investigations du Ministère de la Justice sur le système “Echelon” (nE1745 - Chambre des Représentants -COM 12/01/1999).

Réponse du Ministre :

“Je vous ai dit que le document du Parlement européen , évoqué par votre question , faisait l'objet d'une étude critique par l'administration de la Sûreté de l'Etat et par la Commission pour la protection de la vie privée; que ces services avaient été priés de procéder, le cas échéant, à une enquête plus poussée .

Entre-temps , l'administration de la Sûreté de l'Etat m'a fait savoir “ que l'enquête menée par ses soins n'a pas pu confirmer l'existence et le fonctionnement du système “Echelon”, tout en apportant la nuance que la législation et les moyens d'investigation ne permettent pas à ce service de procéder à des vérifications techniques en ce domaine “

.....”

3.2. Au niveau Européen

La préoccupation des parlementaires belges pour la problématique “Echelon” fait suite à la publication d'une étude intitulée “une évaluation des techniques de contrôle politique”. Cette étude a été menée par la Fondation “Omega” de Manchester à l'initiative du Parlement Européen. Il s'agit d'un document de travail présenté au groupe “Scientific and Technological Options Assesment” (S.T.O.A.) ainsi qu'à “la commission des libertés publiques et des affaires intérieures”.

3.2.1. Le rapport présenté au Parlement européen

L'étude intérimaire intitulée “une évaluation des techniques de contrôle politique”, présente de façon détaillée les systèmes de surveillance globale qui facilitent la surveillance de masse de toutes les télécommunications, y compris le téléphone, les transmissions par fax et par courrier électronique (réseaux nationaux et internationaux d'interception des communications).

La surveillance électronique transatlantique est composée de deux systèmes distincts :

- le système "Echelon" impliquant des services de renseignements tels que le NSA-CIA des Etats-Unis, le GCHQ et MI 6 britanniques;
- le système "UE-FBI" qui assure la liaison entre divers services répressifs .

Selon l'étude :

"Toutes les communications électroniques, téléphoniques et par fax en Europe sont quotidiennement interceptées par la "National Security Agency" des Etats-Unis, qui transfère toutes les informations provenant du Continent européen via le centre stratégique de Londres, puis par satellite vers Fort Meade au Maryland via le centre crucial de Menwith Hill dans la région des North York Moors au Royaume Uni".

"Le système a été mis à jour pour la première fois dans les années soixante-dix par un groupe de chercheurs au Royaume-Uni (Campell, 1981). Des travaux menés récemment par Nicky Hager (Secret Power, Hager, 1996) fournissent des détails extrêmement précis sur un projet nommé "Echelon". Hager a interrogé plus de 50 personnes travaillant dans le renseignement pour découvrir un système de surveillance qui s'étend au monde entier pour former un système pointé sur tous les satellites clés Intelsat utilisés pour transmettre l'essentiel des communications téléphoniques, Internet, le courrier électronique, les télécopies et télex transmis par satellite dans le monde entier. Les sites de ce système sont basés à Sugar Grove et Yakima aux Etats-Unis, à Waihopai en Nouvelle zélande, à Géraldton en Australie, à Hong Kong et à Morwenstow au Royaume-Uni".

"Le système Echelon fait partie du système anglo-américain mais, à l'inverse de nombreux systèmes d'espionnage électronique développés au cours de la guerre froide, "Echelon" vise essentiellement des cibles non militaires : des gouvernements, des organisations et des entreprises dans pratiquement tous les pays. Le système Echelon fonctionne en interceptant sans distinction de très grandes quantités d'informations puis en triant les éléments intéressants à l'aide de systèmes d'intelligence artificielle comme Memex, à la recherche de mots clés. Cinq nations se partagent les résultats, les Etats-Unis faisant figure de partenaire principal en vertu de l'accord UK-U.S.A. de 1948 et la Grande Bretagne, le Canada, la nouvelle-Zélande et l'Australie ayant un rôle subalterne de fournisseurs d'informations. (...)

"Chacun des cinq centres fournit aux quatre autres des "dictionnaires" de mots clés, de phrases, de personnes et de lieux pour "l'identification" et le message intercepté, ainsi identifié est transmis directement au pays demandeur. Parallèlement à la somme d'informations recueillies sur d'éventuels terroristes, il existe une grande part de renseignements à caractère économique, notamment une surveillance renforcée de tous les pays participants aux négociations du GATT. Hager a cependant noté que les principales priorités du système, et de loin, continuent à être le renseignement militaire et politique correspondant aux principaux centres d'intérêt des partenaires du système .

Ce document a été publié le 14 septembre 1998 pour servir de base à la séance de session du mois de septembre 1998.

3.2.2. Résolution sur les relations transatlantiques (système “Echelon”)

Le 16 septembre 1998, le Parlement Européen a adopté la résolution suivante :

“Le parlement européen”

(...)

“Est conscient du rôle crucial que joue la coopération internationale, grâce aux moyens de surveillance électronique, lorsqu’il s’agit de mettre un terme ou d’empêcher les activités des terroristes, des trafiquants de drogue, du crime organisé”;

“Reconnaît toutefois également qu’il est essentiel que l’on puisse s’appuyer sur des systèmes de contrôle démocratique en ce qui concerne le recours à des technologies et les informations obtenues”;

“Demande que de telles technologies de surveillance fassent l’objet d’un réel débat ouvert, tant au niveau national qu’à celui de l’union européenne, et soient soumises à des procédures garantissant une responsabilité sur le plan démocratique”;

“Réclame l’adoption d’un code de conduite destiné à garantir la réparation d’erreurs ou d’abus”;

“Estime que l’importance croissante du réseau Internet, et, plus généralement, des télécommunications à l’échelle mondiale et en particulier le système “Echelon”, ainsi que les risques de leur utilisation abusive appellent l’adoption de mesures de protection des informations économiques et d’un cryptage efficace.” (...)

3.3. Le Parlement français

Le 1^{er} octobre 1998, Monsieur le Sénateur Jacques Legendre a demandé à Monsieur le Premier ministre de lui faire savoir s’il est exact qu’un réseau électronique d’espionnage connu sous le nom “d’Echelon” a été mis en place par les Etats-Unis, la Grande-Bretagne et quelques autres pays anglo-saxons et si ce réseau procède à des écoutes motivées par l’espionnage industriel. Il lui demande quelles mesures le Gouvernement compte prendre pour exiger de nos alliés qu’il soit mis un terme à une action aussi intolérable.

Réponse du Premier ministre :

“..... Cette problématique a plus particulièrement fait l’objet, au début de cette année d’un rapport préparé par le professeur Alain Pompidou, député au Parlement européen et président du groupe d’évaluation des choix technologiques et scientifiques de ce Parlement .

.....

Il n'existe pas d'autorité qui puisse empêcher techniquement , l'interception de communications radioélectriques lorsque celles-ci sont véhiculées dans un espace mondial qui ne connaît pas de frontière physique. Par ailleurs, les enjeux économiques de ces activités sont considérables, compte tenu de l'interconnexion des réseaux de communication avec les systèmes internes des entreprises . Il convient de répondre à ces développements inéluctables au plan des technologies par une politique volontariste dans au moins deux directions . D'une part , le Gouvernement français encourage le développement des moyens permettant de répondre aux besoins de confidentialité et d'intégrité des systèmes d'information sensibles .

.....

L'analyse des risques , le développement des moyens de protection , l'évaluation de la sécurité des systèmes d'information constituent des tâches prioritaires confiées notamment au service central de la sécurité des systèmes d'information du secrétariat général de la défense nationale.

.....

*D'autre part, il est également clair que les investissements consentis pour l'interception des systèmes de communication répondent à des besoins de sécurité et de défense importants . Ceux-ci sont liés, par exemple à la surveillance des activités criminelles ou terroristes, à la prévention et au suivi des crises militaires ou encore à la lutte contre les programmes clandestins de prolifération des armes de destruction massive . Ces sujets présentent un caractère transnational et les Etats recherchent nécessairement, dans ces domaines, des formes nouvelles de partenariat. Le développement de moyens de protection d'un côté , la mise en place d'investissements nécessaires pour faire face à l'essor accéléré des technologies de l'autre , enfin l'établissement de cadres juridiques et de coopération crédibles constituent donc les principales orientations de la politique du Gouvernement dans ces domaines .”
(Sénat français 3 décembre 1998 - Réseau d'espionnage industriel) .*

4. LES SOURCES OUVERTES

D'autres sources ouvertes, tendant à confirmer la pratique des interceptions de télécommunications européennes par les Etats-Unis, ont été consultées par le Comité R. Les quelques articles mentionnés ne sont qu'un bref aperçu de l'innombrable documentation disponible dans les sources ouvertes .

4.1. Zbigniew Brzezinski, ancien conseiller pour la Sécurité Nationale du Président Carter

Dans une interview parue dans le périodique “*Le Nouvel Observateur*” du 10-16 décembre 1998, sous le titre “*Un ancien de la Maison- Blanche brise le tabou. Nous avons fait le choix de tout savoir, Zbigniew Brzezinski, qui fut conseiller pour la sécurité nationale du Président Carter et reste un spécialiste très écouté en matière internationale, est catégorique : oui, l'Amérique espionne le monde entier. Ses amis comme ses ennemis . Et il ne voit rien là d'immoral*”.

Selon Brzezinski :

“...L’Amérique a des responsabilités et des intérêts globaux, mondiaux. Toute nouvelle tendance, tout mouvement imprévu sur la planète peuvent avoir un impact sur son bien-être et sa sécurité. Elle doit donc avoir la capacité d’être renseignée partout, non seulement sur ses ennemis mais aussi sur ses amis .

Le renseignement ne veut pas forcément dire espionnage, au sens classique du terme : le recrutement d’agents. Cette forme de renseignement est risquée, et peut conduire à des scandales très dommageables pour les relations avec le pays ami en question . Mais les écoutes ou l’imagerie spatiale sont, pour ainsi dire, ouvertes, libres et relativement peu risquées. Ces moyens techniques permettent un recueil systématique - et non compromettant - de renseignements . Ils sont plus ou moins à la portée de tout le monde . Chaque pays, selon ses moyens et ses objectifs , décide ou non de les mettre en oeuvre . L’Amérique a fait ce choix . Je pense que le débat éthique sur le renseignement ne se pose vraiment que dans le cas de l’espionnage classique. On peut en effet se demander : le recrutement d’agents est-il une forme appropriée de renseignement à Bonn ou à Paris ? Mais, en matière d’écoutes ou de photos, quelle est la question éthique ? Est-ce immoral de photographier le monde ?”

4.2. Amiral Pierre Lacoste, ancien directeur général de la “Direction générale de la Sécurité Extérieure” (France)

Dans son ouvrage *“Un amiral au secret”* (Flamarion - 1998), l’amiral Pierre Lacoste, ancien directeur général de la “Direction générale de la Sécurité Extérieure”, le service français de renseignements extérieurs déclare : *“Forts du prestige de leur victoire contre l’Empire soviétique, les Etats-Unis mènent avec un exceptionnel dynamisme une politique qui vise à conforter leur situation hégémonique. Leurs stratégies du renseignement s’inscrivent dans cette perspective. Pour valoriser un héritage déjà fort riche en hommes, en moyens techniques et en savoir-faire, ils tirent un profit maximal des nouvelles technologies de l’information et de toutes les opportunités offertes dans les domaines où ils sont en position dominante.*

En raison de leur puissance et de leur vitalité, ils sont sans doute à même, mieux que toute autre nation, de conjurer les dangers liés à l’existence du “second monde”⁽¹⁾, mais, s’ils le font, ce sera dans un cadre qui ressemble plus à une sorte de pax americana qu’à une société de nations partenaires, égales en droits et en devoirs”.

4.3. Martin Brady, directeur du Defense Signals Directorate (DSD - Australie)

Selon un article de Kevin Poulsen publié sur Internet, le directeur du DSD, l’équivalent australien du GCHQ, aurait reconnu dans une lettre rendue publique aux médias le 23 mai 1999, que son service participait au programme d’interceptions réalisées sur l’étranger dans le cadre du programme de coopération UKUSA.

(1) L’amiral Lacoste définit le “second monde” comme étant les structures, soit supranationales, comme l’Union Européenne, soit infranationales, comme les autorités régionales, soit transnationales au profit desquelles les Etats ont perdu, à des degrés divers, une part de leurs attributs.

4.4. Amendement à l'“Intelligence Authorization Act” (E.U.)

Le Comité R a reçu le 2 août 1999 un acte officiel du Sénat Américain :

‘An ACT to authorize appropriations for fiscal year 2000 for intelligence and intelligence -related activities of the United States Government, the Community Management Account , and the Central Intelligence Agency Retirement and Disability System, and for other purposes’ (Senate of the United States, May 18 (legislative day 14, 1999) : ‘sec.307. Report on legal standards applied for electronic surveillance’ où il est mentionné :

“le Directeur de la CIA, le Directeur de la NSA et le département de la Justice doivent transmettre à la Commission appropriée du Congrès un rapport classifié et un non classifié décrivant les bases légales sur lesquelles s’appuie la communauté du renseignement pour réaliser ses différentes interceptions et ses opérations de surveillance électronique”.

Selon le périodique “le Monde du Renseignement” l’amendement aurait été motivé sur base des atteintes au droit constitutionnel des citoyens américains que représenterait “*Echelon*” .

5. CONSTATATIONS À PROPOS DES SERVICES DE RENSEIGNEMENT BELGES

5.1. A la Sûreté de l’Etat

Le Service d’enquêtes du Comité “R” s’est entretenu le 11 février 1999 avec un conseiller général de la Sûreté de l’Etat afin de lui demander quelle était la réaction de ce service de renseignement vis-à-vis de l’existence éventuelle d’un système d’interception des télécommunications dans notre pays par les services spéciaux américains.

De cet entretien il ressort que :

L’existence du système d’interception “*Echelon*” avait été révélé par la presse depuis février 1998.

Les réponses des ministres aux différentes questions et interpellations parlementaires avaient été établies sur base des éléments fournis par l’Administration de la Sûreté de l’Etat elle-même. Ces réponses doivent être correctement interprétées en fonction de la situation de la Sûreté de l’Etat.

A cet égard, trois points doivent être mis en exergue :

- le manque de moyens chronique d’investigations qui, tant sur le plan du personnel que du matériel, ne lui permet pas de vérifier la réalité de l’existence du système “*Echelon*”;

- la Sûreté de l'Etat est totalement étrangère à tout type de recueil de renseignements par satellites et n'a aucun accès à ce type de source d'information.
- la Sûreté de l'Etat ne dispose pas actuellement de législation lui permettant de procéder à des interceptions de sécurité et donc à des écoutes via satellites.

En février 1999, dans une note adressée au ministre de la Justice, la Sûreté de l'Etat précisa à nouveau ne connaître l'existence du système "Echelon" que par le biais de divers articles de presse .

La Sûreté de l'Etat n'entretenait aucune discussion à ce sujet avec le SGR.

5.2. Au SGR

L'information en la possession du SGR n'est issue que de l'examen des sources ouvertes.

Le SGR constate tout d'abord que le système d'intervention des télécommunications "Echelon" lie trois états membres de l'O.T.A.N. et deux autres pays qui ne représentent aucune menace sur le plan militaire.

A l'examen des missions du SGR définies dans la loi organique du 30 novembre 1998 sur les services de renseignements et des restrictions légales sur le captage des radiocommunications, ce service de renseignements n'effectue pas de recherche active sur le programme "Echelon".

Le SGR souligne comme le rapport, intitulé "évaluation des techniques de contrôle politique", publié par le Parlement européen en décembre 1997 le mentionne que :

"bien qu'initialement axé sur des renseignements militaires relatifs à l'Union Soviétique, "Echelon" semble avoir été réorienté, depuis la fin de la guerre froide, sur l'information politique et économique et d'autres sphères d'intérêt, comme le terrorisme ou la criminalité organisée. En effet, puisque les autoroutes de l'information sont de plus en plus utilisées pour l'échange d'informations illégales et pour la coordination d'actions criminelles, "Echelon" est également utilisé pour contrarier les activités de groupements terroristes et maffieux".

Poursuivant son analyse, le SGR jette diverses pistes de réflexion :

"La question "Echelon", aussi importante soit elle, n'est que l'illustration de tout un éventail de menaces auxquelles se voit confrontée notre société de l'information et de la communication. On peut en effet se poser la question de savoir quelle est la valeur d'une telle société sans une protection adaptée aux nouvelles menaces engendrées par un usage intensif de moyens informatiques et de communication. Cette observation nous amène à la problématique de la sécurisation des communications et la protection de l'information contre les menaces liées aux écoutes.

Une des solutions à ce problème est liée à l'usage intensif des moyens de chiffrement forts, un domaine dans lequel le SGR fournit des services au profit d'autres départements".

“Le SGR estime que les implications de ce problème ont pris une telle ampleur qu’il ne serait pas exagéré de les situer au niveau des intérêts fondamentaux du pays, qui peuvent être définis par le Roi, sur proposition du Comité Ministériel (loi organique du 30 novembre 1998 - art. 11-1E)”.

“De plus, il semble évident que cette problématique requiert une approche interdépartementale”.

Par le biais du Ministre de la Défense nationale et en concertation avec la Sûreté de l’Etat, le SGR a récemment attiré l’attention des autorités politiques sur la problématique de la sécurisation des réseaux informatiques”.

6. AUTRES RAPPORTS RÉDIGÉS POUR LE GROUPE STOA

Après réception du rapport du Service d’enquêtes, le Comité R a pris connaissance de diverses études datant d’avril et mai 1999 et qui ont été réalisées à la demande du Parlement européen sous le titre :

“Development of surveillance technology and risk of abuse of economic information” .

S Partie 1/4

“The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception . Survey of opinions of experts (Interim Study)”.

Cette étude reproduit les résultats intermédiaires d’un sondage d’opinions d’experts, complétés de recherches et de matériaux analytiques des auteurs. Elle a été réalisée par ZEUS E.E.I.G. dans le cadre d’un projet d’évaluation technologique sur ce thème qui a été mis sur pied par le STOA, en 1998, à la demande du “Committee on Civil Liberties and Internal Affairs’ du Parlement européen”.

Ce projet STOA est un prolongement d’un ancien projet qui a été réalisé à la demande du même “Committee” et qui portait l’intitulé : “An appraisal of technologies of political control “ (voir supra).

S Partie 2/4

“The legality of the interception of electronic communications: A concise survey of the principal legal issues and instruments under international, European and national law”.

Cette étude a été préparée par Dr. Chris Elliott dans le cadre du programme "pour l'évaluation des options scientifiques et technologiques" du Parlement européen.

Cette étude examine la légalité de l’interception de messages électroniques. L’étude tend à la concision et à la brièveté. Elle se focalise sur les instruments tels qu’ils existent et pas sur la manière dont ils ont été réalisés. Elle évite également toute spéculation quant à l’évolution de la législation sur ce plan et des points moraux et éthiques ainsi soulevés.

Les instruments sont considérés selon trois niveaux :

- Conventions internationales;
- Décisions et directives de l'UE;
- Législation nationale (des Etats de l'UE et d'importantes nations tierces) .

La législation sur ce terrain tend à réconcilier trois aspects contradictoires :

- **LE RESPECT DE LA VIE PRIVÉE**

La vie privée est un droit humain fondamental. Les conventions internationales et les lois nationales traitent davantage des droits de la personne physique que de ceux de la personne morale (sociétés).

- **POSSIBILITÉS SUR LE PLAN POLICIER**

L'interception légale de messages est importante pour les services de police et la plupart des pays disposent de procédures légales pour permettre et réglementer leur interception.

- **BESOINS DE COMMUNICATIONS ÉLECTRONIQUES DU MONDE DES AFFAIRES**

La sécurité est d'une importance essentielle pour favoriser la communication électronique dans le monde des affaires et peut donc nécessiter l'utilisation de systèmes cryptographiques, ce qui pourrait entraîner un conflit par rapport aux besoins policiers.

L'étude s'étend au-delà de l'interception et se consacre également à la cryptographie, puisqu'il s'agit d'un moyen important pour contrer l'interception et qui doit être également soumis à un certain degré de contrôle légal. Elle traite également de la législation sur le stockage et le traitement des données à caractère personnel pour autant qu'il s'agisse de la transmission de telles informations ⁽²⁾.

S Partie 3/4

“Encryption and cryptosystems in electronic surveillance : a survey of the technology assessment issues” .

L'objet initial du présent rapport est de décrire les principales techniques permettant aux citoyens, entreprises ou institutions européens, de se préserver, dans une certaine mesure, contre ce qu'on appelle désormais “l'intelligence économique”.

De ce fait, les objectifs de ce rapport sont :

- *rappeler aux Membres du Parlement Européen les risques, concernant la surveillance électronique, inhérents à l'utilisation des moyens modernes de communication;*

⁽²⁾ Traduction libre de l'anglais

- *fournir aux Membres du Parlement Européen un document de référence concernant les technologies de cryptage, et les statuts actuels des démarches de standardisation de ces techniques;*
- *décrire les directions futures possibles en ce qui concerne, tant les communications sécurisées, que les méthodes de surveillance électronique;*
- *donner aux Membres du Parlement Européen une traduction, à la fois précise et claire pour les non-experts, et montrer les implications pratiques, de documents techniques relatifs à la sécurité de l'information, constituant des amendements récents à des organismes de contrôle internationaux;*
- *proposer des options aux Membres du Parlement Européen permettant de préserver les intérêts des citoyens, entreprises et organisations européennes.*

- Partie 4/4

“The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition” .

Dans cette étude, on explique ce que l'on entend par “Communications intelligence” (COMINT). D'autre part, on y aborde le système “*Echelon*”, révélé par la publication du précédent rapport STOA.

Depuis lors, de nouvelles données ont été publiées qui démontrent que le système existerait déjà depuis les années 70 et qu'il aurait été considérablement étendu entre 1975 et 1995. Cette partie contient de nouvelles informations et des preuves écrites concernant “*Echelon*” et l'interception de signaux satellites.

Le Comité R renvoie le lecteur au rapport cité plus haut, qui consacre beaucoup d'attention, à propos de “*Echelon and Comint production*”, notamment à :

- S “ The Watch List “
- S “ New information about Echelon sites and systems “
- S “ Comint and economic intelligence “

Nous citons à cet égard quelques passages importants du rapport :

- L'équipement Comint dont on dispose actuellement, permet d'intercepter, de traiter et d'analyser des informations de tout système de communication moderne à haute capacité auquel il a accès, y compris les niveaux les plus élevés de l'Internet. On peut difficilement se faire une opinion de l'échelle, de la capacité et de la rapidité de certains systèmes. Des systèmes spéciaux ont été construits pour le traitement de messages émanant des sémaphores, des mobilophones et des nouveaux satellites.

- Lors du débat du Parlement européen en 1998 sur "la relation transatlantique/système *Echelon*", le commissaire Bangeman a remarqué au nom de la Commission que :

"Si ce système existait, il constituerait une violation intolérable des libertés individuelles, de la libre concurrence et de la sécurité des nations".

- Ce rapport décrit le cadre dans lequel des renseignements économiquement sensibles recueillis par "*Echelon*", sont diffusés, avec des exemples où des organisations européennes feraient l'objet de surveillance.
- Des fonctionnaires américains ont admis que la NSA recueille des informations économiques, volontairement ou non. L'ancien attaché militaire, le colonel Dan Smith, a travaillé jusqu'en 1993 à l'ambassade américaine de Londres. Il a reçu régulièrement des renseignements Comint de Menwith Hill.

En 1998, il a déclaré à la BBC au sujet de Menwith Hill :

"Lorsque des communications sont interceptées, il est inévitable, étant donné la large bande utilisée, que des conversations ou des messages soient interceptés qui n'ont rien à voir avec le domaine militaire et qui contiennent probablement des renseignements de nature commerciale."

Sur le plan technique, tout est possible. Toutes ces informations, sur un plan technique, peuvent être recueillies et explorées pour déterminer ce que l'on souhaite précisément. Mais il n'existe aucune directive pour le faire spécifiquement dans l'intérêt d'une entreprise déterminée."

- Le rapport mentionne encore :

En général, cette explication n'est pas inexacte. Elle fait toutefois l'impasse sur la différence qui existe entre "donner une mission" et "la diffusion" et également entre intérêts commerciaux et économiques. Il n'existe aucune preuve que des entreprises du Royaume-Uni ou des Etats-Unis soient en mesure de confier des missions d'interception Comint qui serviraient leurs propres intérêts. Elles n'ont pas non plus besoin de le faire. Dans chacun de ces pays, les services de renseignement nationaux et certains ministères sont officiellement autorisés à confier, sur le plan économique, des missions et à recevoir des renseignements du Comint. De tels renseignements peuvent être recueillis pour de multiples raisons : une évaluation du futur prix de produits indispensables, la détermination de l'attitude d'un pays déterminé durant des négociations commerciales, la surveillance du commerce international des armes, le suivi de technologies sensibles, l'évaluation de la stabilité politique et/ou de la force économique d'un pays déterminé. Chacun de ces objectifs peut fournir des renseignements présentant un intérêt commercial direct. La décision de diffuser ou d'utiliser ces renseignements n'est pas prise par les organisations Comint, mais par les autorités nationales.

- En 1970, le 'US Foreign Intelligence Advisory Board' a ordonné, selon son ancien 'Executive Director' que, "dorénavant les renseignements économiques doivent être considérés comme un élément de la sécurité nationale, présentant une importance aussi grande que des renseignements de nature militaire, diplomatique et technologique".

Le 5 mai 1977, il a été décidé lors d'une réunion entre la NSA, la CIA et le "Department of Commerce", la constitution d'un nouveau département secret : "l'Office of Intelligence Liaison". Sa tâche consistait à traiter des "renseignements étrangers" qui étaient importants pour le "Department of Commerce".

La constitution de cette organisation signifiait PAR CONSEQUENT qu'il existait un mécanisme officiel qui permettait d'utiliser des données NSA pour servir des intérêts commerciaux et économiques.

Après qu'en 1993, un programme télévisé britannique a mis en lumière l'existence de ce système, la dénomination a été changée en "Office of Executive Support".

En 1993, le Président Clinton a également étendu la communication de renseignements à des organisations commerciales par la constitution d'un nouveau "Economic Council", qui travaillait en parallèle avec le "National Security Council".

- Une grande publicité a été faite sur la nature de cette communication de renseignements. D'anciens officiers de renseignement et d'autres experts indiquent que des tuyaux qui résultent d'activités d'espionnage... passent régulièrement du "Commerce Department" à des sociétés américaines pour les aider à engranger des contrats à l'étranger.
- Au Royaume-Uni, le GCHQ a pour mission légale spécifique d'intercepter des communications étrangères "dans l'intérêt du bien-être économique du Royaume-Uni... qui sont en rapport avec des activités ou des intentions de personnes situées en dehors des îles britanniques". Selon un ancien haut fonctionnaire du JIC, les renseignements Comint comprennent de manière routinière des "plans de sociétés, des télex, des fax et des conversations téléphoniques sous forme dactylographiées.
- En Australie, des informations Comint commercialement pertinentes sont transmises par le DSD au "Office of National Assessments", qui détermine alors si et où elles doivent être transmises. Le personnel peut transmettre des renseignements à des entreprises australiennes s'il estime qu'une puissance étrangère fait ou veut faire de la concurrence déloyale.
- Des systèmes analogues sont opérationnels dans les autres pays U.K./USA, soit le Canada et la Nouvelle-Zélande.

Dans le rapport, on trouve enfin plusieurs recommandations (issues) politiques pour le Parlement européen.

- Sur le plan technique, les mesures de protection devraient être orientées vers la lutte contre des activités Comint hostiles par le refus d'accès, ou lorsque cela est impossible ou peu pratique, sur l'impossibilité du déchiffrement des messages par un cryptage généralisé.
- Comme le groupe SOGIS au sein de la Commission l'a reconnu, les intérêts divergents des nations constituent un problème complexe. Les grands Etats ont fortement financé des systèmes Comint. L'un des Etats membres est actif dans l'accord UK/USA, tandis que d'autres sont des "tiers parties" ou ont conclu des accords bilatéraux avec la NSA. De tels problèmes sont à la base de conflits internes et internationaux. Des solutions techniques ne sont pas disponibles.

Il devrait être possible de trouver un intérêt conjoint dans l'imposition de mesures pour lutter contre les activités Comint étrangères futures, orientées contre des Etats européens, leurs citoyens et leurs intérêts commerciaux.

- Une deuxième cause manifeste de conflit est le souhait des Etats "de faire de l'interception de communications dans un cadre policier". Les procédures techniques et légales de l'interception dans un cadre policier et l'interception de communications en vue de recueillir des renseignements sont fondamentalement différentes.

Lorsque l'on ne fait aucune distinction entre les conditions d'une interception aux objectifs policiers et une interception aux intentions de renseignement clandestin, les libertés civiles sont fortement compromises. Il est essentiel pour la protection des droits de l'homme et des libertés fondamentales de faire cette distinction.

- Actuellement, les internet-browsers et d'autres logiciels utilisés dans presque tous les PC en Europe sont manipulés volontairement pour que les communications "sécurisées" qu'ils envoient, si elles sont interceptées, puissent être déchiffrées sans aucun problème par la NSA. Les fabricants américains sont tenus de le faire dans le cadre des dispositions américaines dans le domaine de l'exportation. Il est important que les règles du jeu soient les mêmes pour tout le monde. On pourrait envisager une contre-mesure par laquelle, dans le cas où des systèmes cryptographiques manipulés sont vendus en dehors des Etats-Unis, il deviendrait obligatoire d'utiliser un "standard ouvert" afin que des tiers et d'autres nations puissent prévoir des applications supplémentaires afin de mettre le niveau de la protection, au moins, au même niveau que celui auquel ont droit les consommateurs américains.
- Il est grand temps que le processus actuel de prise de décisions politiques fasse l'objet d'une discussion publique et parlementaire dans les Etats membres de l'UE et au Parlement européen afin que l'on puisse trouver un équilibre entre la sécurité et la vie privée des citoyens et des entreprises commerciales, entre les intérêts financiers et techniques des opérateurs de réseaux de communications et les "service providers", d'une part, et le besoin d'appui aux activités policières dans la lutte contre le crime organisé et le terrorisme, d'autre part ⁽³⁾.

7. L'INTERCEPTION DE COMMUNICATIONS PAR D'AUTRES PUISSANCES QUE LES ETATS-UNIS

D'autre part, il ressort également du rapport précité et d'autres sources ouvertes que d'autres pays disposent également des mêmes possibilités techniques.

Le Comité R cite à cet égard quelques exemples :

⁽³⁾ Traduction libre (partie 4/4) du texte anglais

7.1. Espionnage : Alliance franco-allemande

Le monde du renseignement nE 337 du 18 juin 1998 stipule que :

“Dans un article très documenté paru dans l’hebdomadaire “Le point” du 6 juin, le journaliste très spécialisé Jean Guisnel, auteur notamment d’un ouvrage qui fait autorité, “Guerres dans le cyberspace” révèle que la France et l’Allemagne ont passé un accord pour écouter les satellites civils Intelsat et Immarsat au-dessus du territoire américain. Ces écoutes sont notamment réalisées à partir de la base spatiale de Kourou, en Guyane. “Le point” ajoute que la France a également ouvert récemment une station d’écoutes en Nouvelle-Calédonie, et confirme qu’une station d’interception satellitaire a été construite aux Emirats arabes unis, suite à l’accord en matière de renseignement signé entre les deux pays en 1995.

Selon nos informations, il est probable que l’accord avec l’Allemagne aille encore plus loin, et comprenne le partage des écoutes clandestines effectuées à partir des “grandes antennes” installées dans les ambassades des deux pays”.

7.2. France : Opidium pour se défendre contre Echelon

Répondant à une question écrite d’un sénateur à propos du “réseau électronique d’espionnage connu sous le nom d’Echelon”, le premier ministre français Lionel Jospin vient d’admettre que l’existence d’une coopération internationale associant les Etats-Unis, la Grande-Bretagne, le Canada, l’Australie et la Nouvelle Zélande dans un but éventuel d’espionnage industriel “constitue depuis plusieurs mois un sujet de préoccupation publique”. Il précise qu’il “n’existe pas d’autorité qui puisse empêcher, techniquement, l’interception de communications radioélectriques lorsque celles-ci sont véhiculées dans un espace mondial qui ne connaît pas de frontière physique”. Lionel Jospin ajoute que le gouvernement français a décidé de répondre à “ces développements inéluctables” par une “politique volontariste”. Il révèle ainsi que pour “répondre aux besoins de confidentialité et d’intégrité des systèmes d’information sensible”, le secrétariat d’Etat à l’Industrie a lancé un rappel à projets intitulé OPIDIUM (offre de produits de sécurisation pour la mise en oeuvre des autoroutes de l’information).

Cependant, le gouvernement français ne met pas uniquement l’accent sur l’aspect défensif, et le développement de mesures offensives apparaît clairement dans la réponse de Lionel Jospin.

Celui-ci affirme qu’il est “clair que les investissements consentis pour l’interception des systèmes de communications répondent à des besoins de sécurité et de défense importants. (Voir supra point 3.3 : le parlement français).

7.3. Ecoutes : Bientôt de grandes oreilles en Suisse

Selon "le Monde du Renseignement", le département suisse de la Défense a officiellement annoncé la décision, votée à l'unanimité par le Conseil fédéral, de doter le pays d'un système d'interception des communications par satellites. Le projet d'un coût estimé à plusieurs dizaines de millions de francs suisses, comportera l'achat, à partir de cette année, de neuf antennes paraboliques. Deux antennes d'un diamètre de 18 m seront installées par la société Swisscom sur son site de Loèche. La prestation de Swisscom "se limitera aux domaines de la planification, de la construction, de l'exploitation technique et de l'entretien". Sept autres antennes, de 4 et 13 m de diamètre, seront positionnées sur un site militaire existant dans la région de Heimenschwand. Contrairement à ce qu'a affirmé le journal SonntagsZeitung, il est invraisemblable que ces antennes participent au réseau mondial d'écoutes Echelon.

Comme l'a indiqué le Département de la Défense, "en captant les émissions radio des systèmes étrangers de communications, le Groupe des renseignements de l'armée procure aux autorités civiles et militaires des informations significatives pour la politique de sécurité".

8. CONCLUSIONS

Alors qu'il existait encore un doute en 1998 lors du débat au Parlement européen quant à l'existence du système Echelon, il ressort des études ultérieures, réalisées pour le groupe STOA, que le système "Echelon" serait une réalité. Ce rapport décrit également, sur la base d'exemples, comment des informations économiquement sensibles relatives notamment aux organisations européennes seraient recueillies et diffusées.

D'autre part, il ressort également du rapport précité et d'autres sources ouvertes que d'autres pays disposent également des mêmes possibilités technologiques (voir supra point 7).

Le "communications intelligence (Comint)", qui consiste à effectuer de l'interception dissimulée de communications est utilisée par la plupart des nations modernes depuis que les télécommunications internationales existent.

Les objectifs des opérations Comint sont variés. La plupart des objectifs traditionnels Comint sont les messages militaires et les communications diplomatiques entre les capitales nationales et les missions étrangères. Depuis les années soixante, parallèlement à la croissance du commerce mondial, la collecte de renseignements et d'informations économiques relatifs aux évolutions scientifique et technique est devenue un aspect de plus en plus important du Comint. Les objectifs plus récents comprennent le trafic de drogue, le blanchiment d'argent, le terrorisme et la criminalité organisée.

Une fois qu'il existe un accès aux canaux de communication internationaux pour un but déterminé, l'on a automatiquement accès à tout autre type d'information passant par le même canal. La description de la mission des services constitue la seule restriction en cette matière.

Les services de renseignements belges n'ont pas la possibilité technique de constater eux-mêmes l'existence du système "Echelon". Leur connaissance du sujet résulte de la consultation de sources ouvertes.

La Sûreté de l'Etat n'a pas été en mesure de confirmer l'existence de pratiques d'interceptions de télécommunications. Ce service se déclare confronté à un manque de moyens tant sur le plan personnel que sur le plan matériel. Ses moyens d'investigation ne lui permettent donc pas de vérifier l'existence du système "Echelon".

Le Service Général de Renseignement et de Sécurité considère quant à lui l'existence d'un système d'interception de type "Echelon" comme un fait acquis. Le SGR, représenté au sein du Collège du Renseignement et de la Sécurité, se propose de contribuer aussi bien à la conception des structures fédérales qu'à l'établissement d'une politique générale en matière de sécurisation des réseaux informatiques.

Le SGR n'effectue cependant pas de recherche active sur le programme "Echelon", se fondant, d'une part, sur le fait qu'il ne s'agit pas d'une de ses compétences définies dans la nouvelle loi organique du 30 novembre 1998 sur les services de renseignements et, d'autre part, sur les restrictions légales en matière de captation des radiocommunications.

La loi organique du 30 novembre 1998 des services de renseignements, en son article 7, assigne cependant une mission spécifique à la Sûreté de l'Etat : *"rechercher, analyser et 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, le potentiel scientifique et économique défini par le Comité ministériel, ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Comité ministériel"*.

Une démarche de sensibilisation des entreprises, des administrations et du monde politique à la sécurité des informations paraît donc bien être l'une des missions que le Comité ministériel du renseignement pourrait confier à la Sûreté de l'Etat.

Enfin, il faut encore souligner que l'approche d'une problématique comme "Echelon" doit être située dans un contexte européen.

9. RECOMMANDATIONS

Le Comité R a dû constater dans cette étude de contrôle qu'il n'y avait aucun contact entre le SGR et la Sûreté de l'Etat au sujet de cette problématique : en effet, les deux services avaient uniquement connaissance du "Système Echelon" par l'intermédiaire des sources ouvertes. Le Comité estime qu'un bon échange d'informations obtenues via des sources ouvertes est indispensable et éviterait du travail inutile aux deux services.

Vu la nouvelle mission de la Sûreté de l'Etat, à savoir : *"rechercher, analyser et traiter le renseignement relatif à toute activité qui menace ou pourrait menacer le potentiel scientifique et économique défini par le Comité ministériel, ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Comité ministériel"*, le Comité R proposait déjà dans son rapport d'activités de 1998 :

“Le Comité R préconise, pour réaliser cet objectif, la création d’un organe de concertation entre les ministres concernés et les entreprises détentrices d’un potentiel scientifique ou économique ou d’un intérêt vital pour la Belgique.”

Le Comité R prône que cet organe de concertation serve de lieu de rencontre où la Sûreté de l’Etat sensibiliserait les entreprises, les universités aux menaces en provenance de l’étranger et qu’il serve de lieu d’échange d’informations entre les entreprises, les universités et les services de renseignement ⁽⁴⁾.

Le Comité R estime que la sensibilisation des entreprises aux risques d’interceptions de leurs communications pourrait être un thème de travail au sein de cet organe de concertation.

Si la Sûreté de l’Etat veut assumer cette nouvelle mission correctement, elle devra pouvoir disposer des moyens nécessaires (budgétaires, humains, matériels et techniques) à cet égard.

Dans son rapport d’activités de 1996, le Comité R a publié une étude sur l’interception des communications. Elle y signalait également des réactions du monde politique en la matière.

Dans ses conclusions et recommandations, le Comité R indiquait notamment :

“Ayant en vue l’efficacité des services de renseignements, le Comité ne peut qu’approuver la volonté de leur conférer des possibilités légales d’écoute et d’interception de télécommunications. Ayant en vue la protection des droits des personnes, le Comité ne peut accepter ce moyen de recueillir le renseignement sans l’assortir de garanties rigoureuses et de modalités de contrôle.

Ce point de vue s’appuie :

S sur l’article 8 de la Convention européenne des droits de l’homme, ainsi que sur la jurisprudence de la Cour européenne des droits de l’homme;

S sur la recommandation du Conseil de l’Europe pour la protection de la vie privée” ⁽⁵⁾.

Dans son rapport d’activités de 1997, le Comité R faisait mention d’une étude de contrôle au sujet de :

“L’écoute éventuelle de communications téléphoniques et l’interception de communications par le SGR”.

⁽⁴⁾ Comité R - rapport d’activités - 1998 - deuxième partie - B - chapitre 1 - p. 102

⁽⁵⁾ Comité R - rapport d’activités - 1996 - titre II - chapitre 2 - pp. 47 et 48

Dans ses recommandations, le Comité R répétait :

“qu’il s’est prononcé 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 à ce propos (voir supra) “⁽⁶⁾.

Jusqu’à ce jour, un premier pas a été franchi en matière d’interception de communications par les services de sécurité et de renseignement, puisque la loi organique des services de renseignement et de sécurité du 30 novembre 1998 prévoit en son article 44 :

*“L’article 259bis du Code pénal est complété par un § 5 rédigé comme suit :
les dispositions du § 1^{er}, 1° en 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.”*

Lorsque le Comité R répète ici cette recommandation, il renvoie à la réponse, visée plus haut, du Premier Ministre français à une question parlementaire (voir supra point 3.3) .

Comme en France, il semble au Comité R recommandé de répondre de manière double à la problématique résultant des nouvelles évolutions technologiques :

- d'une part, il faut accorder de l'attention à la protection des systèmes d'informations,
- d'autre part, il est clair que l'interception de communications par les services de renseignement est une nécessité, notamment en vue de la prévention et du suivi des crises militaires, de la lutte contre le commerce clandestin des armes, et dans le cadre de la lutte contre les activités criminelles ou terroristes...

Le Comité R estime que pour lutter contre le phénomène d’activités Comint illégitimes, il faudra accorder encore beaucoup plus d’attention à la sécurité des systèmes d’information.

La résolution parlementaire européenne de 1978 relative au ‘Transatlantic/ECHELON system’ exigeait des "mesures de protection sur le plan des informations économiques et de l’efficience de l’encryptage".

Dans le rapport visé plus haut, réalisé pour le groupe STOA (partie 4/4), l’on mettait encore l’accent à titre de recommandation pour le Parlement européen sur l’impossibilité de déchiffrer les messages par un encryptage généralisé comme mesure de protection contre des activités Comint hostiles.

⁽⁶⁾ Comité R - rapport d’activités - 1997 - deuxième partie - B - chapitre 1 - section 3 - p. 99

Le Comité R soutient dès lors la position du SGR qui est d'avis que concernant la problématique de la sécurisation des communications et la protection de l'information contre les menaces liées aux écoutes, une des solutions est liée à l'usage intensif des moyens de chiffrement forts, un domaine dans lequel le SGR fournit des services au profit d'autres départements .

Le SGR défend l'idée d'une sensibilisation du Collège du Renseignement et de la Sécurité ainsi que des autorités politiques par le biais notamment du Comité ministériel du renseignement afin de dégager des axes de prévention à l'échelle nationale tant dans le secteur public que privé.

Le Comité R rappelle d'ailleurs que dès 1996, il avait recommandé l'élaboration et la mise en oeuvre d'une réglementation en matière de sécurité des systèmes d'information : *"Il s'agit là 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 renseignement et avec quels moyens"*⁽⁷⁾.

Enfin, il faut encore mentionner qu'en Belgique, par la loi du 19 décembre 1997, l'utilisation de la cryptographie est libre. C'était une première en Europe.

Le Comité R souhaite une fois encore mettre l'accent sur le fait que pour réaliser les objectifs précités, tant la Sûreté de l'Etat que le SGR devront pouvoir disposer en suffisance d'un personnel qualifié.

⁽⁷⁾ Comité R - rapport d'activités - 1996 - Titre V - Recommandations - chapitre 2 p. 225

LEXICON

* * * * *

Définition : 'Source Ouverte'

Dans son rapport d'activités 1996 le Comité R a défini les sources ouvertes comme suit :

"les sources qui, d'un point de vue éthique ou légal, sont accessibles au public moyennant paiement ou non".

(rapport d'activités 1996 - Titre III - Chapitre 3 - p. 208).

BND : *Bundesnachrichtendienst (Allemagne - Duitsland)*

CIA : *Central Intelligence Agency (USA)*

CSE : *Canadian Communications Security Establishment - provides the Government of Canada with foreign Sigint Intelligence*

DGSE : *Direction Générale de la Sécurité Extérieure (France - Frankrijk)*

DSD : *Defense Signals Directorate (Australia)*

FBI : *Federal Bureau of Investigation, the National Law Enforcement and Counter-intelligence agency of the USA*

GCHQ : *Government Communications Headquarters - the Sigint- agency of the UK*

GCSB : *Government Communications Security Bureau (New Zealand)*

INTELSAT : *International Telecommunications Satellite*

JIC : *Joint Intelligence Committee (UK)*

LMR: *Le Monde du Renseignement , périodique bimensuel édité en français et en anglais par le groupe INDIGO PUBLICATIONS, Paris, France*

MI6 : *Secret Intelligence Service (UK)*

NSA : *National Security Agency USA, the Sigint Agency of the USA*

STOA : *Science and Technology Options Assessment of the European Parliament*

UKUSA : *United States of America., United Kingdom , Canada, Australia and New Zealand (UK-USA agreement)*

La NSA et le GCHQ ont conclu en 1948 un accord secret , les unissant avec le CSE Canadien.

Le DSD australien , puis le GCSB néo-zélandais ont rejoint le consortium, qui travaille sur le renseignement politique et militaire, sur le trafic de drogue, le terrorisme et sur le monde économique .

B. A L'INITIATIVE DU COMITE R

CHAPITRE 1 : RAPPORT SUR LE SUIVI PAR LE SGR DES RECOMMANDATIONS SUR LE RWANDA FORMULÉES PAR LA COMMISSION D'ENQUÊTE PARLEMENTAIRE

1. MOTIFS ET OBJET DE L'ENQUÊTE

Dans son rapport d'activités 1996, le Comité R a relevé les lacunes des services de renseignement à propos des événements au Rwanda en 1994⁽¹⁾. "*L'absence d'un service de renseignements sur place et d'une capacité d'analyse efficace*" fut épinglée par la suite par la Commission parlementaire d'enquête ⁽²⁾.

Cette carence visait non seulement la structure mise en place dans le cadre de la mission de l'ONU, mais aussi plus particulièrement celle du bataillon belge.

Les déficiences au niveau de la collecte des informations avaient de surcroît été aggravées par l'absence d'un traitement efficace par le SGR qui n'avait pas pu produire d'analyse pertinente permettant au gouvernement belge de préparer une politique tenant compte des circonstances réelles présentes sur le terrain des opérations. Les causes de cette carence étaient attribuées à un manque d'effectifs et de flexibilité, à une trop grande importance accordée à la source des informations plutôt qu'au contenu de celles-ci et à l'inexistence du retour d'information.

Compte tenu de ces éléments et des recommandations formulées par la Commission parlementaire, il est apparu essentiel au Comité R de vérifier dans quelle mesure il avait été tenu compte de ces dernières.

2. PROCÉDURE

Le 5 mai 1998, le Comité R a ouvert une enquête sur la manière dont le SGR avait donné suite aux recommandations de la Commission parlementaire d'enquête sur les événements du Rwanda.

Deux membres du Comité R furent désignés pour suivre cette enquête et faire rapport.

(1) Comité R - rapport d'activités - 1996 - pp. 120 à 136

(2) Rapport de la Commission parlementaire -1997/1998 - 1-611/7- Point 4.6 - pp. 711, 712 et 721

Les Présidents de la Chambre des représentants et du Sénat furent avertis par lettres du 12 mai 1998, de l'ouverture de cette enquête, en application de l'article 46, 3° du règlement d'ordre intérieur du Comité R.

Le 19 mai 1998, une apostille a été envoyée au chef du Service d'enquêtes du Comité R.

Le Ministre de la Défense nationale fut pour sa part informé de l'ouverture de cette enquête par un courrier du chef du Service d'enquêtes daté du 2 juin 1998, conformément à l'article 43.1 de la loi organique du 18 juillet 1991 sur le Contrôle des services de police et de renseignements.

Le Service d'enquêtes du Comité R a transmis son rapport à ce dernier le 8 mars 1999.

Le Comité R a approuvé le présent rapport le 20 juillet 1999.

3. LE SUIVI DES DIFFÉRENTES RECOMMANDATIONS

Le Comité R a vérifié comment ces recommandations ont été appliquées dans les dernières opérations menées par les forces armées belges à l'étranger.

3.1. Les mesures prises par le SGR en matière de collecte du renseignement

La Recommandation 29 du rapport de la Commission parlementaire d'enquête stipule que le contingent belge doit toujours disposer d'un réseau de renseignement solide qui lui soit propre, composé d'officiers de renseignements suffisamment formés et maîtrisant, si possible, la langue du pays. A défaut, on doit disposer en permanence d'interprètes dignes de confiance.

Il est actuellement prévu qu'une équipe du SGR accompagne chaque contingent des forces armées belges d'une certaine importance envoyé en opération à l'étranger. La décision est prise en fonction des circonstances et en concertation avec l'Etat-Major Général. La présence d'un détachement avancé du SGR sur le terrain doit permettre un retour rapide d'informations exploitables.

La composition de l'équipe dépend notamment :

- du besoin en information à récolter par des moyens propres au SGR,
- des possibilités de récolte d'information par moyens techniques ou humains,
- du risque encouru par le déploiement de telles équipes,
- de la disponibilité des moyens en personnel et en matériel.

En tout état de cause, les détachements du SGR sur le terrain comprennent au moins un analyste chargé de l'exploitation des renseignements. Dans la mesure du possible, le SGR envoie des agents connaissant la langue locale ou l'anglais; à défaut, il a recours à des interprètes dont il vérifie la fiabilité.

A l'heure actuelle, les officiers et agents de renseignement reçoivent surtout leur formation sur le terrain. Ils suivent également des stages de formation. La question de la formation fait actuellement l'objet d'études au sein du SGR en vue de dispenser à l'avenir aux nouvelles recrues, une formation structurée et préalable à leur prise de fonction effective.

A l'exception des officiers de la force aérienne où le renseignement (élargi parfois au contrôle aérien) constitue une spécialité, il n'existe pas de possibilité de carrière continue dans le domaine du renseignement militaire au sein du SGR. La force terrestre a opté, en effet, pour une approche plus polyvalente dans la gestion de son personnel. Toutefois, un effort a été engagé et se poursuit pour une spécialisation d'une partie du personnel de renseignement en fonction des besoins.

Des instructions provisoires sont d'application pour les missions en cours; elles seront évaluées en fonction de leur application sur le terrain pour permettre l'élaboration d'ordres permanents.

Cet objectif ne pourra toutefois être réalisé qu'après une augmentation des effectifs du SGR permettant notamment d'affecter du personnel à la formation sans pour autant porter préjudice au fonctionnement normal du service.

3.2. Les mesures prises par le SGR en matière d'analyse, d'évaluation et de diffusion du renseignement

Le point 30 du rapport de la commission d'enquête sur le Rwanda stipule que le SGR doit disposer de suffisamment d'analystes qui évalueront le contenu de chaque information. En outre, il doit y avoir un retour d'information systématique à l'adresse des unités sur le terrain. Pour rappel, il était apparu, en effet, qu'à l'époque des événements du Rwanda, un seul analyste était affecté à l'analyse des données en relation avec la situation sur place.

3.2.1. *Du personnel d'analyse*

Le SGR a récemment procédé au recrutement de nouveaux analystes civils et militaires; leur nombre doit encore augmenter prochainement. Toutefois, on estime que le cadre actuel de ces analystes ne permet pas encore l'accomplissement optimal des missions du SGR.

Les analystes sont affectés à des domaines et à des régions du monde nécessitant une analyse continue en fonction des priorités nationales. Pour les autres régions et domaines, le SGR collabore avec des services de renseignement étrangers alliés. En effet, il faut être conscient que le SGR ne pourra jamais couvrir toutes les régions du monde dans tous les domaines du renseignement. La spécialisation de tous les analystes n'est donc pas l'orientation du SGR. Ce service se doit de disposer surtout d'analystes généralistes ayant une grande capacité de rassembler rapidement des informations, de les sélectionner, de les analyser et d'en faire une synthèse dans différents domaines. Il s'agit en effet de pouvoir faire face aux demandes imprévues concernant des régions n'ayant pas la priorité du SGR.

En ce qui concerne leur qualification, leur statut et leur recrutement, il faut faire une distinction entre les analystes militaires et les analystes civils.

Les militaires ont une formation universitaire ou d'ingénieur en même temps qu'ils disposent d'une formation spécifique au corps d'armée dont ils proviennent. Il s'agit d'officiers de carrière, mais il est parfois fait appel à des officiers de réserve. Le choix des analystes est déterminé en fonction de leur disponibilité, de leur expérience dans un domaine particulier du renseignement ou de leur connaissance des régions du monde qu'ils seront amenés à traiter. Bien qu'il ne soit pas maître de la gestion du personnel, le SGR essaye de recruter sur une base volontaire après un contact préalable avec le candidat. Les mutations imposées vers le SGR sont quasi exclues.

Les civils sont de niveau universitaire. Actuellement, ils sont recrutés sur base contractuelle après une première sélection des candidatures réalisée d'après les diplômes et les compétences particulières qui détermineront leur zone d'emploi. Cette sélection est suivie de tests de connaissances et de tests psychotechniques organisés par le SGR. Le recrutement s'effectue sur base des résultats obtenus, et après une interview réalisée par le chef du SGR qui décide en dernier ressort.

Un nouveau statut des agents civils du SGR est en cours d'élaboration. Ce statut offrira aux analystes civils des possibilités d'avancement en instaurant les grades de commissaire divisionnaire et de commissaire du service de renseignement.

3.2.2. De l'évaluation du contenu des informations.

Dans le cadre des événements du Rwanda, la Commission parlementaire avait épinglé le fait que l'on ne s'était basé que sur une source unique d'informations.

Pour répondre concrètement à cette critique, le SGR a développé le principe du recoupement des informations. Les règles à suivre sur la manière d'évaluer le contenu de chaque information font partie de la formation générale des analystes et sont reprises dans tous les cours sur le sujet.

Pour assurer le caractère contradictoire des analyses, des échanges de vue entre analystes du SGR sont organisées, de même que des réunions avec le ministère des Affaires étrangères et des échanges de vue avec des services de renseignement étrangers.

La confrontation des analyses du SGR et de celles de la Sûreté de l'Etat s'effectue également dans la mesure où les domaines de responsabilité convergent.

Le recoupement des informations lors du processus d'exploitation permet de juger de la fiabilité des sources, ainsi que de la crédibilité des informations. Ce système permet éventuellement de déceler une possible manipulation.

3.2.3. De la diffusion de l'information

Les analyses réalisées dans le cadre des missions des forces armées belges à l'étranger sont diffusées à la Maison militaire du Roi, au cabinet du Premier Ministre, aux ministères de la Défense nationale et des Affaires étrangères, à la Sûreté de l'Etat, aux différents Etats-majors des forces armées, aux attachés militaires belges à l'étranger ainsi qu'aux unités impliquées dans les opérations.

Des informations sont également envoyées aux services de renseignement étrangers avec lesquels le SGR a passé des accords.

Ces analyses sont envoyées en fonction de l'implication de leurs destinataires dans les opérations et de leur besoin d'en connaître.

Des directives concernant le retour des informations à destination des unités du terrain sont en cours d'élaboration. Lorsqu'il concerne la protection du contingent belge, ce retour d'information doit se faire le jour même. Lorsqu'il s'agit d'informations moins urgentes, la durée du retour est de 48 heures environ.

3.3. Le fonctionnement du SGR

Le point 36 du rapport de la Commission parlementaire sur le Rwanda stipule que le SGR doit devenir un instrument efficace et cohérent de soutien pour les responsables des opérations, tant au niveau de l'Etat-Major général que pour les responsables sur le terrain. Il y est également précisé que le SGR doit être informatisé et pouvoir fonctionner avec rapidité, précision et souplesse.

Les moyens matériels, notamment informatiques, dont dispose actuellement le SGR semblent lui permettre de remplir sa mission de manière satisfaisante.

Pour recueillir l'information nécessaire à la préparation et à l'exécution de ses missions, le SGR collabore avec la Sûreté de l'Etat (voir l'enquête concernant le protocole d'accord conclu entre ces deux services), les services de renseignement des pays de l'OTAN et ceux des pays étrangers avec lesquels un accord bilatéral a été conclu.

Le point 37 du rapport de la Commission parlementaire d'enquête sur le Rwanda indique que le SGR doit pouvoir renforcer les unités déployées sur le terrain dans le domaine du renseignement, notamment par la mise à disposition d'équipes de personnel spécialisé ou par des moyens techniques.

Ces derniers visent entre autres les moyens de captation de communications dont dispose le SGR pour pouvoir répondre aux besoins de nouvelles missions d'appui direct aux troupes belges engagées dans les opérations de maintien de la paix.

Une étude est en cours au SGR afin de déterminer l'orientation future à suivre dans ces domaines, en tenant compte de la nouvelle loi organique sur les services de renseignement, des recommandations de la Commission parlementaire sur le Rwanda et de nos engagements internationaux.

Il convient de rappeler à ce sujet que l'article 44 de la nouvelle loi du 30 novembre 1998⁽³⁾ organique des services de renseignement et de sécurité prévoit que les dispositions du § 1^{er}, 1^o et 2^o de l'article 259 bis du Code pénal, 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."

L'étude précitée doit aboutir à un programme de remplacement du matériel existant par du nouveau matériel susceptible d'être déployé rapidement sur le terrain lors d'une opération impliquant des troupes belges.

3.4. Autres mesures

3.4.1. Structure et personnel du SGR

Le SGR fait l'objet d'une restructuration visant à améliorer son fonctionnement. Le projet de nouvelle structure a été adopté et une demande d'adaptation du tableau organique du personnel permettant l'application de cette nouvelle structure a été faite auprès de l'Etat-Major général.

Le Comité R a été informé de ce projet et il continuera à l'être au fur et à mesure de sa mise en application.

Pour l'exécution de ce projet, le SGR dépend de la hiérarchie militaire et du pouvoir politique. Les deux ont donné clairement une priorité à l'augmentation des capacités du SGR. Le SGR considère les recommandations de la Commission parlementaire comme un défi auquel il essaye de répondre le plus rapidement et le mieux possible.

Toutefois, la réalisation des projets envisagés demandera des délais incontournables inhérents à la mise en place et à la formation du personnel supplémentaire, à la création de nouvelles infrastructures, etc

3.4.2. L'analyse d'images satellitaires

Le Comité R avait recommandé pour sa part de mettre en place au SGR un centre d'analyse d'images satellitaires et de former du personnel qualifié à cette fin, ce qui devait signifier la mise en oeuvre de moyens matériels et humains adéquats ⁽⁴⁾.

En octobre 1998, le gouvernement a décidé de créer un centre national d'interprétation d'images satellitaires pour les besoins nationaux et d'en faire une compétence exclusive du SGR. En effet, la vocation principale du Centre de Torrejón étant de préparer des dossiers au profit du Conseil de l'UEO, ceci implique l'impossibilité pour la Belgique de programmer ses recherches de façon indépendante.

(3) M.B. 18/12/ 1998 - p. 40.312

(4) Comité R - rapport d'activités - 1998, pp. 130 à 177.

Le centre belge travaillera avec des images commerciales et avec d'autres images, en vertu d'accords opérationnels.

L'état-major des forces armées a élaboré un plan d'action concernant ce centre en termes de personnel, de timing, de fonctionnement et de budget sur lequel le ministre de la Défense nationale a marqué son accord. Un budget a été prévu à cet effet dans la tranche 1999 du Plan à Moyen Terme de la Défense.

4. CONCLUSIONS

Le Comité R a pu constater que le Service Général de Renseignement et de Sécurité déploie de nombreux efforts afin de rencontrer les préoccupations de la Commission parlementaire et ce, quel que soit le secteur de ses responsabilités : renseignements, protection du bataillon, analyse, feed-back, transmissions etc

Cet effort s'inscrit dans un contexte concret d'opérations en cours, alors que le SGR est lui-même en restructuration interne.

Le souhait du SGR est d'assurer une formation adéquate et approfondie des analystes récemment engagés. Toutefois, les contraintes subsistent et ce souci légitime quant à la formation doit s'intégrer dans les priorités imposées au SGR de plus en plus souvent sollicité par le pouvoir politique et la situation mondiale préoccupante.

Il convient enfin de souligner que les conclusions de l'enquête de contrôle confirment ce qui est repris à propos du fonctionnement du Service de renseignements et de sécurité (SGR), dans la note de politique générale du Gouvernement sur la participation belge aux opérations de maintien de la paix du 28 janvier 1998 ⁽⁵⁾.

A plusieurs reprises, et malgré les efforts déjà accomplis en ce sens, il a toutefois été constaté que le SGR était confronté à un problème chronique de moyen en personnel l'obligeant à faire des choix en fonction des nécessités immédiates.

⁽⁵⁾ Sénat 1-859/1 et Chambre 1394/1 - 97/98, pp. 12 et 13

CHAPITRE 2 : RAPPORT SUR LA MISE EN APPLICATION DU “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”.

1. INTRODUCTION

Le 20 février 1997, sous l’impulsion conjointe des Ministres de la Justice et de la Défense nationale, l’Administrateur général de la Sûreté de l’Etat et le Chef du SGR contresignaient un protocole d’accord visant à *“améliorer la collaboration entre les services de renseignement par la coordination de leurs activités dans les domaines du renseignement, de la sécurité, de la technique, de l’échange de documents et d’informations, de l’échange d’idées et d’analyses et de la résolution d’éventuels conflits de compétence, en vue d’optimiser l’utilisation des moyens limités consacrés au renseignement et à la sécurité.”*

Ce protocole a pris force exécutoire le 1^{er} avril 1997.

2. PROCEDURE

En date du 1^{er} octobre 1998, le Comité R décide, d’initiative, dans le cadre de sa mission légale de contrôle et dans la foulée des conclusions et recommandations de son rapport consacré à *“l’efficacité et à la collaboration des services de renseignement à la lumière des événements dramatiques survenus au Rwanda”* ⁽¹⁾ d’ouvrir une nouvelle enquête d’évaluation de la collaboration et de la coordination entre services de renseignement, plus particulièrement axée sur l’application du Protocole d’Accord précité qui, à cette époque, lie les services co-signataires depuis 18 mois. Il s’agit donc essentiellement de prendre, après une période suffisante de rodage, la mesure de la coopération qui devrait s’être installée entre services.

Il échet de rappeler ici qu’à cette date du 1^{er} octobre 1998, la loi organique des services de renseignement et de sécurité, actuellement en vigueur, n’est pas encore publiée. Celle-ci dispose désormais en son article 20 § 1 que *“les services de renseignement et de sécurité...veillent à assurer entre eux une coopération mutuelle aussi efficace que possible...”*, et au § 3 que *“le Comité Ministériel définit les conditions...de la coopération prévue au § 1^{er}...”*

(1) Comité R - rapport d’activités - 1996 - pp. 120 à 136

Une apostille est délivrée en ce sens au chef du Service d'enquêtes en date du 5 octobre 1998, le priant de "procéder à l'audition des responsables et de vérifier leurs déclarations". Dès le 7 octobre 1998, conformément à l'article 46.3 du règlement d'ordre intérieur, la présidente du Comité R avise les Présidents du Sénat et de la Chambre de la mise en oeuvre de cette enquête.

En exécution de l'article 43.1 de la loi du 18 juillet 1991, les ministres de la Justice et de la Défense nationale se voient à leur tour informés, en date du 12 octobre 1998, du démarrage de l'enquête.

Un questionnaire est élaboré par le Service d'enquêtes et adressé aux services de renseignement fin novembre 1998.

Les mémoires en réponse seront réceptionnés le 25 janvier 1999 pour la Sûreté de l'Etat et le 2 mars 1999 pour le SGR. Les auditions (conjointes) des responsables désignés par le Général Simons et par l'Administrateur général Monsieur B. Van Lijsebeth se sont déroulées en date des 8 et 15 mars 1999.

Le présent rapport a été approuvé le 6 août 1999.

3. INTERET PARLEMENTAIRE

Le Comité R n'a pas relevé d'interpellation ou de question parlementaires englobant précisément l'exécution réservée par les services au Protocole d'Accord. Il n'est toutefois pas inintéressant de relever ici que parmi les *sujets* inscrits à l'ordre du jour du Protocole, révélant à ce titre le souci de coordination accrue entre services en la matière, certains ont fait l'objet de très nombreuses questions et interpellations parlementaires.

4. CONSTATATIONS

Les réunions communes sont conjointement organisées sur une base semestrielle, entre spécialistes des services, en exécution de l'article 16 du protocole. Il semble bien, tant à la lecture des documents remis qu'à l'issue des auditions réalisées par le Service d'enquêtes du Comité R, que toutes les réunions proposées aient eu lieu, pour la plupart aux dates envisagées.

Toutefois des comptes-rendus de ces réunions ne sont pas automatiquement rédigés, ne contiendraient-ils encore que l'identité des participants, la matière traitée et les conclusions tirées. Les responsables des services apprécient donc au cas par cas l'opportunité de dresser ou non des procès-verbaux.

Le Comité R a pu constater, sur base de la documentation fournie et des auditions auxquelles il a été procédé, l'existence de contacts réguliers entre services. Les procès-verbaux de réunions produits témoignent de la réalité d'une collaboration par ailleurs qualifiée d'excellente lors des auditions. En résumé, aux dires des uns et des autres le protocole serait parfaitement appliqué. Il y a complémentarité.

Si l'on affine quelque peu l'analyse, on constate que le calendrier révèle un taux fluctuant de fréquence des réunions et échanges de documents suivant la période de référence mais surtout en raison de la matière considérée.

C'est ainsi qu'en ce qui concerne le secteur des activités relatives aux sectes nuisibles, espionnage, extrémisme idéologique, crime organisé, prolifération et terrorisme, certaines problématiques ayant fait l'objet d'une attention renouvelée de la part du monde politique, et notamment du gouvernement, des informations sont également échangées à d'autres niveaux. Un exemple est donné : la cellule administrative de coordination de la lutte contre les sectes nuisibles ⁽²⁾ présidée par le Ministre de la Justice, au fonctionnement de laquelle a été associée - notamment - la Sûreté de l'Etat.

Par ailleurs le SGR comme la Sûreté de l'Etat participent au Comité de Coordination interdépartemental pour la lutte contre les transferts illégaux d'armes, en abrégé C.I.T.I. ⁽³⁾, lequel se réunit trimestriellement sous la présidence collégiale des délégués des ministres du Commerce Extérieur et des Affaires Etrangères.

Le Comité R constate que les forums de rencontre entre services se sont multipliés; que les contacts directs et personnels semblent abondamment utilisés dans les matières requérant un ajustement rapide; que le réflexe de la collaboration est unanimement présenté comme solidement enraciné dans les domaines d'intérêt commun; que le principe-même des réunions conjointes est, aux dires de chacun, bien rôdé et que la règle de communication des informations au service "pilote" ne paraît avoir engendré ni frustrations ni récriminations, au contraire. Il ne semble donc pas y avoir de contentieux entre les services de renseignement sur la coordination et la collaboration visées au protocole. Les deux services jettent un même regard satisfait sur leur propre exécution de celui-ci, mais également sur celle de leur partenaire.

5. RECOMMANDATIONS

Puisque la collaboration est décrite comme fructueuse par l'un et l'autre services, le Comité R ne peut recommander - sur un plan général - que la persistance de celle-ci, et son extension à d'autres matières non expressément visées au protocole, de sorte à aboutir à terme à une véritable "culture de collaboration".

Le Comité R regrette cependant que des comptes-rendus de réunions communes ne soient pas systématiquement rédigés. Il y va non seulement d'un manque de rigueur sur le plan méthodologique mais également d'une atteinte à la possibilité de contrôle.

Le Comité R préconise donc qu'à l'avenir des procès-verbaux soient systématiquement rédigés à l'issue des réunions communes.

⁽²⁾ Loi du 02.06.1998 (M.B. 25.11.1998) et A.R. du 08.11.1998 (M.B. 09.12.1998)

⁽³⁾ A.R. du 09.02.1999 (M.B. 26.05.1999)

Il se propose dans l'avenir, dans le cadre élargi de la loi organique des services de renseignement et de sécurité du 30 novembre 1998 et des futures directives du Comité ministériel du renseignement et de la sécurité, d'examiner dans chaque secteur d'activités de quelle manière se maintient cette collaboration destinée à optimiser l'utilisation des moyens.

CHAPITRE 3 : L'INTERVENTION DE LA SÛRETÉ DE L'ETAT DANS LES PROCÉDURES DE NATURALISATION AINSI QUE DANS LE CADRE DE LA LOI SUR L'ACCÈS AU TERRITOIRE, LE SÉJOUR, L'ÉTABLISSEMENT ET L'ÉLOIGNEMENT DES ÉTRANGERS

1. INTRODUCTION

Un document daté du 21 août 1997, élaboré par la Sûreté de l'Etat dans le cadre de la publicité active de l'administration, mentionne "*la communication de renseignements en rapport avec les demandes de naturalisation*" comme l'une des missions de ce service.

D'autre part, comme mentionné dans le titre II - D. les plaintes - du présent rapport d'activités 1999, le Comité R a été saisi de deux plaintes introduites par deux ressortissants étrangers.

Ceux-ci demandaient en outre à pouvoir prendre connaissance des données que la Sûreté de l'Etat avait transmises aux autorités compétentes suite au refus de la commission des naturalisations de la Chambre des représentants de leur octroyer la nationalité belge.

Un des plaignants souhaitait ainsi pouvoir introduire une nouvelle demande et s'expliquer sur les faits rapportés à son sujet par la Sûreté de l'Etat.

Le Comité R qui ne dispose pas de la compétence légale d'ouvrir aux particuliers l'accès à leurs dossiers auprès des services de renseignement, a pour le surplus constaté l'absence d'atteinte aux droits des plaignants.

Le Comité R a cependant souhaité ouvrir cette enquête d'ordre général afin de mieux connaître l'intervention de la Sûreté de l'Etat dans l'application de diverses mesures légales à l'égard des étrangers.

Le Comité R a donc examiné les échanges d'informations qui existent en cette matière entre la Sûreté de l'Etat d'une part, l'Office des étrangers, les autorités judiciaires et le Parlement d'autre part pour en rechercher les fondements légaux.

2. PROCÉDURE

Le 24 septembre 1998, le Comité R a décidé de mener une étude sur le sujet.

Le 13 octobre 1998, le Comité R a décidé de transformer cette étude en enquête : il a adressé une apostille à son Service d'enquêtes le même jour.

Le 15 octobre 1998, en application de l'article 46, alinéa 3 du règlement d'ordre intérieur, les présidents de la Chambre des représentants et du Sénat ont été informés qu'une enquête était en cours sur *"l'intervention de la Sûreté de l'Etat dans les procédures de naturalisation d'une part, dans le cadre de la loi sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers d'autre part"*.

Le 16 octobre 1998, en application de l'article 43 alinéa 1^{er} de la loi organique du 18 juillet 1991, le Ministre de la Justice a été informé de l'ouverture de cette enquête par le chef du Service d'enquêtes.

Les 11 décembre 1998 et 8 janvier 1999, le Ministre de l'Intérieur a été informé de l'ouverture de cette enquête, le Comité R souhaitant faire l'inventaire des courants d'échanges d'informations qui existent entre la Sûreté de l'Etat et l'Office des étrangers.

Le Comité R souhaitait également être informé de l'état d'avancement d'un projet d'accord entre ces deux services.

L'Administrateur général de la Sûreté de l'Etat ainsi que le Directeur général de l'Office des étrangers, ont été informés de cette intention du Comité R par lettres du 11 décembre 1998.

Le Service d'enquêtes du Comité R a mené son enquête au cours des mois de janvier, février et mars 1999. Le rapport d'enquête a été déposé au Comité R le 12 avril 1999.

Au cours des mois de mai et juin 1999, le Comité R a sollicité quelques informations complémentaires auprès de la Sûreté de l'Etat, de l'Office des étrangers et du Collège des médiateurs fédéraux.

Le présent rapport, destiné à la publication, a été approuvé par le Comité R le 7 juillet 1999.

3. L'INTÉRÊT PARLEMENTAIRE

Si de nombreuses questions parlementaires ont été récemment posées sur l'application des lois dont il est question dans la présente enquête, l'intervention de la Sûreté de l'Etat dans cette matière n'est que très rarement évoquée.

Sur ce sujet, le Comité R n'a relevé que la question suivante posée en 1989 :
Question n° 133 de M. Nols du 6 janvier 1989 (Questions & Réponses- Chambre, 1988-1989, p. 3992) concernant l'activité d'agents de la sûreté au sein de milieux étudiants zaïrois.

Le Comité R n'a pas connaissance d'autres questions ou d'interpellations parlementaires faisant référence aux notions "d'ordre public" et de "sécurité nationale" (ou "sûreté de l'Etat") dans la législation relative aux étrangers.

Ces notions furent cependant évoquées en commission du Sénat lors de la discussion générale d'une proposition de loi "*visant à réduire la durée de la détention administrative des étrangers en séjour illégal sur le territoire belge*"⁽¹⁾.

4. HISTORIQUE DES ÉCHANGES D'INFORMATIONS ENTRE L'OFFICE DES ÉTRANGERS ET LA SÛRETÉ DE L'ETAT

Jusqu'au 31 décembre 1993, l'Administration de la Sûreté publique du Ministère de la Justice se composait de la Sûreté de l'Etat d'une part, de l'Office des étrangers d'autre part.

Jusqu'alors, existait une interpénétration naturelle entre ces deux services d'où résultait un échange intensif d'informations entre eux. Les demandes de renseignements se déroulaient le plus souvent de manière orale (par téléphone) et informelle.

En 1974, une note interne de la Sûreté de l'Etat définissait la mission de ce service à l'égard des étrangers comme étant une mission de "*police des étrangers sur le plan politique*".

Dans le cadre de cette mission, la Sûreté de l'Etat exerçait une surveillance très étendue des activités politiques exercées par des étrangers en Belgique.

Par la suite, la problématique de l'immigration n'a plus été perçue comme un problème de sûreté publique. L'étranger a cessé d'être considéré comme un subversif potentiel et d'ailleurs, celui-ci dispose en Belgique des mêmes libertés d'opinion et d'expression que les citoyens belges.

Depuis le 1^{er} janvier 1994, en application d'un arrêté royal du 31 décembre 1993, toutes les compétences relatives à l'accès au territoire, au séjour, à l'établissement et à l'éloignement des étrangers, y compris les compétences du Commissariat général aux réfugiés et aux apatrides et celles de la Commission permanente de recours des réfugiés ont été confiées au ministre de l'Intérieur.

Au 1^{er} janvier 1994, l'Office des étrangers a donc été transféré au Ministère de l'Intérieur, alors que l'Administration de la Sûreté de l'Etat est restée attachée au Ministère de la Justice.

Tout lien organique a donc disparu entre la Sûreté de l'Etat et l'Office des Etrangers.

Néanmoins, cette nouvelle situation n'a pas fondamentalement modifié les relations qui existaient entre les deux services; des informations ont continué à être échangées entre eux. A défaut d'un cadre légal précis, ces nombreux contacts se sont déroulés de manière informelle.

(1) Sénat : 1 / 911 / 4 - 15/12/1998

Au cours des années, l'Office des étrangers a quelque peu formalisé sa manière d'adresser des demandes d'informations à la Sûreté de l'Etat; celles-ci doivent dorénavant être introduites par écrit.

De même, l'Office des étrangers a entrepris de rédiger un projet d'accord avec la Sûreté de l'Etat pour régler ces relations; toutefois, en l'absence de cadre légal à cette époque, ce projet n'a pas abouti.

Depuis juin 1998, la Sûreté de l'Etat a désigné un officier de liaison auprès de l'Office des étrangers, ce qui a eu pour conséquence d'améliorer le contrôle et l'efficacité des échanges d'informations entre ces deux services.

Depuis lors, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, est entrée en vigueur le 1^{er} février 1999.

5. LES MOTIFS D'ÉCHANGES D'INFORMATIONS ENTRE L'OFFICE DES ÉTRANGERS ET LA SÛRETÉ DE L'ÉTAT

La loi du 30 novembre 1998 "*organique des services de renseignement et de sécurité*"⁽²⁾, entrée en vigueur le 1^{er} février 1999, définit à présent les missions générales des services de renseignement.

Cette loi contient aussi des dispositions réglementant le recueil de données par ces services:

Article 14 : "Dans le respect de la loi, sur la base des accords éventuellement conclus ainsi que des modalités déterminées par leurs autorités compétentes, les autorités judiciaires, les fonctionnaires et les agents des services publics peuvent communiquer d'initiative au service de renseignement et de sécurité concerné les informations utiles à l'exécution de ses missions.

A la requête d'un service de renseignement et de sécurité, les autorités judiciaires, les fonctionnaires et les agents des services publics peuvent, dans le respect de la loi, sur la base des accords éventuellement conclus ainsi que des modalités déterminées par leurs autorités compétentes, communiquer au service de renseignement et de sécurité concerné les informations utiles à l'exécution de ses missions".

Cette même loi régit également la communication par les services de renseignement de données à caractère personnel à des autorités et services publics : de telles données ne peuvent être communiquées que "*conformément aux finalités de leurs missions*" (article 19).

Cette nouvelle loi fixe donc les missions générales de la Sûreté de l'Etat mais elle ne prévoit pas explicitement le rôle que ce service peut jouer dans l'application des législations relatives aux étrangers.

⁽²⁾ M.B. 18/12/1998 - p.40.312

L'article 7, § 1^{er}, 4^o dispose seulement que ce service peut être chargé *“d'exécuter toutes autres missions qui lui sont confiées par ou en vertu de la loi”*.

Les commentaires du gouvernement sur ce projet d'article indiquent :

“Le § 1^{er}, 4^o, vise des missions qui sont ou seraient confiées à la Sûreté de l'Etat par ou en vertu de lois particulières. Par exemple, (...) la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, la loi du 3 janvier 1933 relative à la fabrication, au commerce et au port des armes, et au commerce des munitions (...)”⁽³⁾.

Avant l'entrée en vigueur de la loi du 30 novembre 1998, le Comité R avait dénombré quatre matières à propos desquelles la Sûreté de l'Etat et l'Office des étrangers s'échangeaient des informations.

Outre les deux lois citées dans le commentaire du gouvernement, on trouve aussi la loi du 28 juin 1984 *“relative à certains aspects de la condition des étrangers et instituant le Code de la nationalité belge”*⁽⁴⁾ ainsi que certaines mesures d'application de l'article 28 de la loi du 29 mai 1959 relative à l'enseignement (pacte scolaire).

Le Comité R a donc recherché dans les conventions internationales ainsi que dans les lois précitées, les dispositions particulières sur base desquelles peut se justifier l'intervention de la Sûreté de l'Etat dans la mise en oeuvre de mesures administratives ou législatives à l'égard de ressortissants étrangers.

Compte tenu de ce qu'une des missions générales attribuées à la Sûreté de l'Etat par la loi organique précitée est notamment la recherche du renseignement relatif à toute menace contre la sûreté intérieure et extérieure de l'Etat et les relations internationales, le Comité R a spécialement retenu les dispositions faisant référence à *“l'ordre public”*, à la *“sécurité nationale”* ou la *“sûreté de l'Etat”*.

5.1. Les Conventions internationales

L'application des lois précitées doit être conforme aux normes et conventions internationales suivantes :

- la *“Convention internationale du 28 juillet 1951 relative au statut des réfugiés”* (approuvée par la loi du 26 juin 1953);
- la *“Convention internationale du 28 septembre 1954 relative au statut des apatrides”* (approuvée par la loi du 12 mai 1960);
- la *“Convention européenne d'établissement et le protocole du 13 décembre 1955”* (approuvée par la loi du 24 mars 1961) ;

⁽³⁾ Chambre des représentants - 638 / 1 - 95 / 96 - s.o. 2 juillet 1996, p. 10.

⁽⁴⁾ Cette loi a été modifiée, notamment par les lois des 13/06/ 1991, 06 /08/1993, 13/04/ 1995, 20/12/1995 et, dernièrement par la loi du 22/12/1998.

- l' "Accord de Schengen du 14 juin 1985" entre cinq pays de l'Union Européenne relatif à la suppression graduelle des contrôle aux frontières communes, et sa "Convention d'application du 19 juin 1990" en matière de contrôle frontalier et de coopération policière et judiciaire (approuvés par la loi du 18 mars 1993).

De manière générale, ces conventions fixent les conditions dans lesquelles chaque Etat contractant accepte de recevoir des ressortissants étrangers (y compris des réfugiés et des apatrides) sur son territoire, ainsi que les droits dont ces personnes disposent.

Dans le cadre de l'Union européenne, il existe aussi des directives du Conseil des ministres en matière de déplacement et de séjour par lesquelles chacun des Etats membres a le devoir de faciliter l'entrée sur son territoire des ressortissants des autres Etats membres et à leur permettre d'y circuler librement et d'y résider de manière prolongée ou permanente.

C'est ainsi que sept pays de l'Union européenne ont signé à Schengen un accord ayant pour but de réaliser "la suppression des contrôles aux frontières communes dans la circulation des personnes et d'y faciliter le transport et la circulation des marchandises".

Cependant, toutes ces conventions prévoient aussi que des mesures de restriction à l'accès au territoire (expulsion, éloignement) ou à la jouissance de certains droits (liberté de circulation ou d'établissement, etc ...) peuvent être prises pour des raisons d'ordre public, de sécurité de l'Etat, de défense nationale ou de santé publique.

De même, la convention d'application de l'accord de Schengen organise les mesures, les procédures et les règles communes qui garantissent la protection de l'ensemble du territoire des sept Parties Contractantes.

Enfin, des motifs intéressant la sûreté de l'Etat peuvent s'opposer à ce que des raisons d'ordre public qui sont à la base d'une décision relative à un étranger soient portées à sa connaissance.

5.2. L'échange d'informations en vue de l'application de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers

5.2.1 Les mesures de restriction à l'accès au territoire, au séjour et à l'établissement des étrangers

La loi du 15 décembre 1980 ne contient aucun article obligeant de manière explicite l'Office des étrangers à consulter la Sûreté de l'Etat pour des cas spécifiques.

Cette loi suggère cependant de manière indirecte la pertinence des contacts entre ces services dans les cas où des raisons d' "ordre public" et de "sécurité nationale" justifient que le ministre de l'Intérieur prenne des mesures de sûreté à l'égard d'étrangers.

Ces mesures de restriction à l'accès au territoire, au séjour et à l'établissement des étrangers sont les suivantes :

- S le refoulement aux frontières (articles 3 et 52bis) ;
- S l'ordre de quitter le territoire (article 7) ;
- S le refus d'autorisation de séjour de plus de trois mois (articles 9 à 13) ;
- S le refus d'établissement dans le Royaume (article 15, alinéa 4) ;
- S le renvoi et l'expulsion (articles 20) ;
- S l'ordre donné à un étranger de quitter des lieux déterminés, d'en demeurer éloigné ou de résider en un lieu déterminé (article 22) ;
- S le refus d'entrée et de séjour à un étranger ressortissant d'un pays de la Communauté européenne (article 43) ;
- S le refus de laisser un étranger ressortissant d'un pays de la Communauté européenne entrer dans le royaume pour y présenter ses moyens de défense dans le cadre d'une procédure en révision (article 44) ;
- S la non-communication des raisons d'ordre public ou de sécurité justifiant ces mesures (articles 23 et 46) ;
- S l'assignation à résidence et la mise à la disposition du Gouvernement des candidats réfugiés (article 54 §2) ;
- S la détention administrative (articles 7, alinéa 6, 25, alinéa 6, 29, alinéa 4, 74/5, §3, alinéa 3, 74/5, §4, 3°, et 74/6, §2, alinéa 3).

5.2.2. Le modus Operandi

Une directive du ministre de la Justice datée du 22 avril 1986 ("*Instructions relatives à la politique à suivre concernant le séjour d'étrangers - procédures applicables et règles à prendre en considération*") indique que la Sûreté de l'Etat doit être consultée avant l'octroi d'un visa ou d'un permis de séjour aux ressortissants de certains pays.

Ce service doit par ailleurs communiquer à l'Office des étrangers les informations qu'elle possède sur des étrangers dont le séjour en Belgique entraîne une menace pour l'ordre public et / ou la sécurité de l'Etat.

5.2.3. La constatation des infractions à la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers

Autrefois, l'article 81 de cette loi du 15 décembre 1980 disposait que :

*"(...) les infractions à la présente loi sont recherchées et constatées par tous les officiers de police judiciaire, en ce compris ceux dont la compétence est limitée, par les sous-officiers de la gendarmerie, **par les agents de l'administration de la Sûreté publique** et de l'Administration des douanes et accises, par les inspecteurs du Ministère de l'Emploi et du Travail et du Ministère des Classes moyennes ainsi que par ceux de l'Office national de la sécurité sociale".*

Suite au transfert de l'Office des étrangers au ministère de l'Intérieur, cet article 81 a été modifié par la loi du 15 juillet 1996 : les agents de l'Office des étrangers ont donc repris cette compétence d'officier de police judiciaire autrefois dévolue aux agents de l'administration de la Sûreté publique, dont faisait alors partie la Sûreté de l'Etat.

5.2.4. La commission consultative pour les demandes de régularisation

Le 4 octobre 1998, le Conseil des Ministres a décidé d'installer une commission consultative pour les demandes de régularisation.

Cette commission est chargée de donner un avis motivé sur la demande de régularisation, chaque fois que le Ministre de l'Intérieur ou la "Cellule Régularisations spéciale permanente" en fait la demande.

Ceci est notamment indiqué lorsqu'il y a des doutes au sujet de l'application des critères de régularisation que peuvent demander certains étrangers en situation illégale en Belgique.

La circulaire du 15 décembre 1998 ⁽⁵⁾ précise qu'il peut être demandé à la commission consultative de rendre un avis au sujet d'un dossier individuel, *"par exemple, dans un dossier concret où il peut y avoir un doute quant à l'évaluation du danger pour l'ordre public"*.

La circulaire en question n'indique cependant pas de quelle manière la commission consultative est informée des éléments qui lui permettent d'évaluer le danger pour l'ordre public ou éventuellement, la sécurité nationale.

L'intervention de la Sûreté de l'Etat n'est nullement évoquée à ce propos.

La Sûreté de l'Etat a fait savoir au Comité R qu'à ce jour (juin 1999), elle n'avait encore jamais été consultée par la Commission consultative pour les demandes de régularisation des sans-papiers.

⁽⁵⁾ M.B. - 19 /12/ 1998 - p.40.492

5.3. L'échange d'informations en vue de l'application de la loi du 28 juin 1984 relative à certains aspects de la condition des étrangers et instituant le Code de la nationalité belge

L'acquisition de la nationalité belge par un étranger est possible de plusieurs manières : elle suppose soit une déclaration ou une option de l'intéressé faite devant l'officier de l'état civil, soit une demande de naturalisation adressée à la Chambre des représentants.

On ne trouve pas dans la loi de 1984 une référence explicite aux notions d' "*ordre public*" ou de "*sûreté de l'Etat*".

Il est seulement mentionné que le procureur du Roi peut s'opposer à l'acquisition de la nationalité belge par déclaration ou par option "*s'il y a un empêchement résultant de faits personnels graves*" (articles 12bis et 15 §2) ou "*s'il y a des raisons (...) d'estimer que la volonté d'intégration du déclarant est insuffisante*". Ces faits ou ces raisons doivent être précisés et l'acte d'opposition doit être motivé.

En pareille circonstance, le tribunal de première instance statue sur le bien-fondé de l'opposition. La vérification de la volonté d'intégration est menée par le parquet au moyen d'une enquête confiée à la police communale.

En principe, ce n'est pas le rôle de la Sûreté de l'Etat de fournir un quelconque élément d'appréciation sur la volonté d'intégration du demandeur.

Jusqu'il y a peu, l'intervention de ce service dans les procédures d'acquisition de la nationalité belge n'était évoquée que dans l'exposé des motifs de ces dispositions ⁽⁶⁾.

Toutefois, dans la pratique, la commission des naturalisations de la Chambre des représentants a pris l'habitude de consulter directement la Sûreté de l'Etat avant de statuer sur les demandes.

La loi du 22 décembre 1998 modifiant le Code de la nationalité belge ⁽⁷⁾ légalise à présent cette consultation directe de la Sûreté de l'Etat.

Cette loi contient en effet une disposition rédigée de la sorte :

*"Lorsque le dossier du demandeur est complet, la Chambre des représentants transmet la demande de naturalisation au parquet du tribunal de première instance de la résidence principale du demandeur, à l'Office des étrangers et **au service de la Sûreté de l'Etat**, pour avis à fournir dans un délai de quatre mois, sur les critères prévus à l'article 19 et les conditions et circonstances prévues à l'article 15, §2, ainsi que sur tout autre élément dont la Chambre souhaite être informée. (...)"* (Article 21, § 3, alinéa 2).

⁽⁶⁾ Doc parl. Sénat de Belgique- session 1994-199/ 1247 - 2 p. 5 : l'exposé des motifs précisait à ce propos que "*le substitut demande alors l'avis de la Sûreté de l'Etat et celui de l'Office des étrangers*."

⁽⁷⁾ M.B. 06/03/1999 - deuxième édition, p. 7265; cette loi est entrée en vigueur le 1^{er} septembre 1999

Les instances consultées devront transmettre un accusé de réception sans délai et, à défaut d'observations dans les quatre mois qui suivent, l'avis sera réputé favorable. La Chambre des représentants statue alors sur l'octroi de la naturalisation selon les modalités déterminées dans son règlement.

Cette même loi modifiant le Code de la nationalité belge attribue une nouvelle compétence à la Chambre des représentants : celle de statuer sur l'octroi de la naturalisation lorsque le demandeur a fait une déclaration de nationalité et que celle-ci a fait l'objet d'un avis négatif du procureur du Roi.

Dans ce cas, la Chambre des Représentants pourra inviter le demandeur à déposer un mémoire en réponse à l'avis négatif. La Chambre pourra aussi charger le parquet, l'Office des étrangers et la Sûreté de l'Etat de procéder dans les deux mois à une enquête complémentaire sur les motifs qui ont fondé l'avis négatif et sur les éléments invoqués par le demandeur dans son mémoire en réponse.

L'obtention de la nationalité belge par la voie de la naturalisation n'est toutefois pas un droit; elle résulte de l'exercice d'un pouvoir souverain reconnu au pouvoir législatif ⁽⁸⁾.

L'étranger ne peut donc obtenir la communication ou la copie de son dossier de naturalisation: l'article 32 de la Constitution aux termes duquel "*chacun a droit de consulter chaque document administratif et de s'en faire remettre copie (...)*" ne vise que l'exécutif, à l'exclusion du législatif et du judiciaire ⁽⁹⁾.

La loi du 22 décembre 1998 modifiant le Code de la nationalité belge ne remet pas ce principe en cause mais il permet toutefois à l'étranger de connaître la teneur de l'avis négatif motivé rendu par le procureur du Roi à l'encontre de sa déclaration de nationalité, et ce, de manière à lui permettre de rédiger son mémoire en réponse.

Il n'est cependant pas prévu que l'étranger puisse prendre connaissance des données que la Sûreté de l'Etat a communiquées à l'occasion de sa demande de naturalisation, ni du dossier de l'enquête qu'elle a menée à son sujet.

La communication de ces données personnelles peut en effet se heurter aux exceptions relatives à la sûreté nationale et à la vie privée telles que prévues par la loi du 11 avril 1994 "*relative à la publicité de l'administration*" ⁽¹⁰⁾.

La nouvelle loi du 11 décembre 1998 "*relative à la classification et aux habilitations de sécurité*" est aussi de nature à s'opposer à la communication de telles données.

(8) Cour d'Arbitrage, arrêt n° 75/98 - 24 juin 1998 - Journal des tribunaux, 710/1998.

(9) Civ. Bruxelles (référé) 24 septembre 1997 - Journal des tribunaux 710/1998.

(10) Comité R - rapport d'activités - 1997 - "*Les droits d'accès du particulier à son dossier individuel auprès d'un service de renseignement*", pp. 53 à 73.

5.4. Les compétences de la Sûreté de l'Etat en matière d'armes à l'égard des étrangers

La Sûreté de l'Etat dispose de compétences décisionnelles en matière d'armes à l'égard des étrangers ⁽¹¹⁾.

Ces compétences trouvent leur fondement dans la loi du 3 janvier 1933 relative à la fabrication, au commerce et au port des armes, et au commerce des munitions, ainsi que dans ses arrêtés royaux d'exécution.

Il s'agit de la délivrance des autorisations de détention d'une arme à feu de défense ⁽¹²⁾ et des permis de port d'arme de défense ⁽¹³⁾ aux étrangers qui n'ont pas de domicile en Belgique ainsi qu'aux Belges qui résident à l'étranger.

Selon ces dispositions, le ministre de la Justice ou son délégué (en l'occurrence, la Sûreté de l'Etat) peut aussi suspendre, voire même retirer, une autorisation de détention d'une arme de défense ou de guerre *“s'il apparaît que la détention peut porter atteinte à l'ordre public”*.

Cette décision de suspension ou de retrait doit cependant être motivée.

Outre ses compétences décisionnelles précitées en matière d'armes, la Sûreté de l'Etat délivre également des avis à l'égard d'autres instances chargées de l'application de cette législation, notamment à l'Office des étrangers.

Une instruction donnée par le ministre de la Justice en 1964 priait les commissaires de Police et commandants de Gendarmerie de s'informer auprès de la Sûreté publique (Police des étrangers) de la situation administrative de tout étranger demandeur d'une autorisation d'achat d'une arme ainsi que *“des renseignements défavorables que cette administration posséderait à son sujet”*.

Cette instruction se référait à un rapport du Sénat exprimant l'avis que l'autorisation devait être refusée *“si l'acquisition ne se justifie à aucun titre ou si des circonstances spéciales contre-indiquent l'autorisation, notamment, s'il y a lieu de craindre que le requérant ne veuille faire un mauvais usage de l'arme en Belgique ou à l'étranger ou si son casier judiciaire est chargé”*⁽¹⁴⁾.

Malgré le transfert de l'Office des étrangers au ministère de l'Intérieur, et en l'absence de nouvelles instructions en la matière, ce service a continué à consulter la Sûreté de l'Etat en cas de demande introduite par un étranger résidant en Belgique.

(11) Comité R - rapport d'activités 1998 - *“ Enquête sur les compétences et le fonctionnement du service législation en matière d'armes de la Sûreté de l'Etat ”*, pp.103 à 118.

(12) L'annexe de l'arrêté royal du 20 septembre 1991 modèle N° 4

(13) L'annexe de l'arrêté royal du 20 septembre 1991 modèle N° 5

(14) Sénat Doc. 99, p. 3 - session 1930-1931

En 1998, le Comité R n'avait trouvé aucun fondement légal certain à ces compétences d'avis, si ce n'est le point 5.6.4. de la circulaire coordonnée du 30 octobre 1995 sur les armes à feu. Cette circulaire prescrit en effet qu'une enquête locale doit notamment tenir compte d'une "**éventuelle activité politique violente**".

Le Comité R avait estimé préférable qu'une consultation de la Sûreté de l'Etat soit prévue de manière formelle.

5.5. L'échange d'informations en vue de l'application de la législation relative à l'enseignement

En vertu de l'article 18, 1 de l'arrêté royal du 22 mars 1969, nul ne peut être désigné professeur dans l'enseignement à titre temporaire s'il n'est pas belge ou ressortissant d'un pays membre de l'Union européenne sauf dérogation accordée par le Gouvernement.

La législation sur l'enseignement ne définit aucun critère permettant au gouvernement de justifier son refus d'accorder une telle dérogation de nationalité.

Une telle décision résulte donc d'un pouvoir discrétionnaire accordé au gouvernement. Dans la pratique, cette dérogation peut être refusée pour des raisons de sûreté publique.

Cette compétence appartient à présent aux gouvernements des communautés qui ont néanmoins conservé l'habitude de consulter l'Office des étrangers.

L'Office des étrangers questionne à son tour la Sûreté de l'Etat.

6. CONCLUSIONS ET RECOMMANDATIONS

La nouvelle loi du 30 novembre 1998 "*organique des services de renseignement et de sécurité*"⁽¹⁵⁾ fixe les missions générales de la Sûreté de l'Etat sans toutefois définir le rôle particulier que ce service peut jouer dans l'application des législations relatives aux étrangers.

L'article 7, § 1er, 4° dispose seulement que ce service peut être chargé "*d'exécuter toutes autres missions qui lui sont confiées par ou en vertu de la loi*".

L'exposé des motifs citait donc la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers comme un exemple de ces "*autres missions*".

Pourtant, les références aux notions d' "*ordre public*" et de "*sécurité nationale*" que cette loi contient rendaient déjà pertinent l'échange d'information entre l'Office des étrangers et la Sûreté de l'Etat dans le cadre de sa mission générale de recherche, d'analyse et de traitement du renseignement.

⁽¹⁵⁾ M.B. 18/12/1998 - p.40.312

Parmi les quatre législations examinées dans la présente étude, seule la délégation prévue par la loi du 3 janvier 1933 sur les armes permet de confier à la Sûreté de l'Etat une véritable mission particulière visée à l'article 7, § 1^{er}, 4^o précité.

Il s'agit de la délivrance, du retrait ou de la suspension des autorisations de détention d'une arme à feu de défense et des permis de port d'arme de défense aux étrangers qui n'ont pas de domicile en Belgique ainsi qu'aux belges qui résident à l'étranger.

Aux termes de l'article 14 de la loi du 30 novembre 1998, le recueil d'informations par la Sûreté de l'Etat auprès de l'Office des étrangers doit se faire *“dans le respect de la loi”* et *“sur base des accords éventuellement conclus ainsi que des modalités déterminées par leurs autorités compétentes”*, à savoir les ministres de la Justice et de l'Intérieur.

Un tel accord existe entre les autorités administratives de la Sûreté de l'Etat et l'Office des étrangers. Cet accord est concrétisé par la présence d'un officier de liaison de la Sûreté de l'Etat auprès de l'Office des étrangers; c'est par son intermédiaire que passe l'échange d'informations entre ces deux services.

Toutefois, il n'a pas été porté à la connaissance du Comité R que cet accord ait été entériné par les deux ministres compétents.

Compte-tenu de la disposition précitée, le Comité R estime souhaitable que les modalités de recueil de renseignements de la Sûreté de l'Etat auprès de l'Office des étrangers fassent l'objet d'un accord signé entre les départements ministériels compétents.

Cette même loi organique habilite la Sûreté de l'Etat à communiquer des données personnelles relatives à des ressortissants étrangers aux autorités administratives et judiciaires *“conformément aux finalités de leurs missions”* (article 19).

C'est cette disposition qui permet par exemple de justifier la communication de données aux ministres responsables de l'enseignement à propos de professeurs temporaires de nationalités étrangères qui demandent une dérogation à la condition de nationalité.

Toutefois, cette disposition ne rend pas la consultation de la Sûreté de l'Etat obligatoire comme le fait la nouvelle loi du 22 décembre 1998 modifiant le Code de la nationalité. Cette loi organise en effet la consultation directe de la Sûreté de l'Etat par la Chambre des représentants dans la mise en oeuvre de la procédure de naturalisation.

Le Comité R pense d'ailleurs qu'il ne serait pas inutile que la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers prévoie aussi la consultation de la Sûreté de l'Etat par les autorités compétentes en la matière chaque fois que la notion de *“sécurité de l'Etat”* est en jeu.

Dans aucun cas il n'est prévu que l'étranger puisse prendre connaissance des données personnelles que la Sûreté de l'Etat communique à son sujet à l'Office des étrangers, au parquet ou à la Chambre des représentants dans l'application des lois précitées.

La communication de ces données personnelles se heurte en effet aux exceptions relatives à la sûreté nationale et à la vie privée telles que prévues par la loi du 11 avril 1994 *“relative à la publicité de l'administration”*.

La nouvelle loi du 11 décembre 1998 "*relative à la classification et aux habilitations de sécurité*" est aussi de nature à s'opposer à la communication de telles données.

C. A L'INITIATIVE DU SERVICE D'ENQUÊTES

ENQUETE DE CONTROLE RELATIVE A L'EFFICACITE DU SGR ET A LA COLLABORATION DES DEUX SERVICES DE RENSEIGNEMENT CONCERNANT LE VOL D'ARMES COMMIS A HOUTHULST EN 1997

1. PROCEDURE

Par un courrier du 16 mars 1998, le Service d'enquêtes a notifié au président du Comité R l'existence d'une enquête d'office visant à examiner l'efficacité du SGR concernant le vol d'armes commis au dépôt de munitions militaire de Houthulst.

A la suite de la note précitée du Service d'enquêtes, le Comité R a décidé lors de la réunion du 19 mars 1998 de confirmer l'ouverture de cette enquête et de l'étendre à la collaboration des deux services de renseignement dans cette affaire.

Par un courrier du 20 mars 1998, Messieurs les Présidents de la Chambre et du Sénat, conformément à l'article 46 § 3 du règlement d'ordre intérieur, ont été informés de l'ouverture d'une enquête de contrôle.

Conformément à l'article 43 § 1 de la loi du 18 juillet 1991, le chef du Service d'enquêtes a prévenu le 4 mai 1998 les ministres de la Justice et de la Défense nationale qu'une enquête de contrôle avait été ouverte.

Le 9 juin 1998, le Service d'enquêtes a transmis un questionnaire au chef du SGR.

Le SGR a répondu à ce questionnaire du Service d'enquêtes le 15 septembre 1998.

Le rapport a été approuvé le 6 août 1999 par le Comité R.

2. MOTIF DE L'ENQUETE

Le 23 septembre 1997, il a été constaté qu'un lot important de munitions avait été dérobé par effraction entre le 1^{er} juin 1997 et le 22 septembre 1997 au dépôt de munitions militaire de Houthulst au préjudice du Ministère de la Défense nationale.

A la mi-décembre 1997, cet événement a été commenté en long et en large dans divers médias.

Cet événement a incité également certains parlementaires à interpeller les ministres de la Défense nationale et de la Justice à ce sujet :

- Question (orale) de M. Jean-Paul Moerman du 18 décembre 1997 concernant "*Le vol d'armes commis à Houthulst*" adressée au ministre de la Défense nationale (*Chambre des représentants, 49^e législature - SO 1997/1998 - Annales plénières 18/12/1997*)
- Question nE 746/2 de M. Loones du 30 décembre 1997 concernant le "*Vol au dépôt de munitions de la caserne de Houthulst*" adressée au ministre de la Défense nationale (*Questions et Réponses - Sénat - 3 mars 1998 - nE 1-67*) ;
- Question nE 839/1 de M. Loones du 6 février 1998 concernant le "*Vol au dépôt de munitions de la caserne de Houthulst*" adressée au ministre de la Justice (*Questions et Réponses - Sénat – 17 mars 1998 - nE 1-68*) ;
- Question orale de M. Hostekint du 8 janvier 1998 concernant "*le vol avec effraction au dépôt de munitions de Houthulst et les réformes structurelles qui s'imposent au sein de l'armée*" adressée au ministre de la Défense nationale (*Sénat - Annales parlementaires - Séance du 8 janvier 1998*) ;
- Question orale de M. Hostekint du 12 mars 1998 concernant "*Le vol de munitions à Houthulst*" adressée au ministre de la Défense nationale (*Sénat - Séances plénières - compte rendu analytique du 12 mars 1998*) ;
- Question orale nE 871 de M. Cuyt du 17 mars 1998 concernant "*Le lien éventuel entre le dépôt d'armes des Hells Angels et l'armée belge*" adressée au ministre de la Défense nationale (*Chambre des représentants - 49^e législature - SO 1997-1997 Annales com. 17 mars 1998*).

Ces munitions ont été retrouvées par la gendarmerie le 11 mars 1998 à Waregem dans les milieux des " Hells Angels ".

Le vol a fait l'objet d'une enquête judiciaire. Par jugement du tribunal correctionnel de Gand du 28 avril 1999, plusieurs suspects ont été condamnés, notamment pour ce vol; cette affaire serait toujours pendante devant la Cour d'appel.

3. NORMES EN VIGUEUR

3.1. "L'instruction sur la sécurité militaire" (IF 5)

"L'instruction sur la sécurité militaire – IF 5" a été réalisée et diffusée par le SGR, après approbation du chef de l'Etat-major général.

L'édition revue et adaptée du règlement IF 5 publiée en 1997 peut être qualifiée, en ce qui concerne les forces armées, de "bible" dans le domaine de la sécurité.

Pour la réalisation de cette nouvelle édition, il a été tenu compte de la législation en vigueur au 1^{er} décembre 1996.

Cette instruction est basée sur les textes légaux, les directives ministérielles, les règlements, les ordres généraux et autres directives, qui trouvaient leur origine dans des conventions interalliées.

Elle présente la politique de sécurité générale en vigueur pour et au sein de nos forces armées, et détermine la manière d'appliquer cette politique dans la pratique.

Cette instruction a été complétée par deux autres règlements, à savoir :

IF 5bis – *Partie 1* : "Normes de sécurité pour les bâtiments et installations militaires"

IF 5bis – *Partie 2* : "Directives et normes pour la mise en pratique de la sécurité des systèmes d'information (INFOSEC)".

"Le règlement IF 5 a pour but :

1. de compiler tous les principes et règles permanents dont l'application est nécessaire pour obtenir un niveau de sécurité militaire maximal et cela, pour tous les organismes militaires belges à l'intérieur et à l'extérieur du pays;
2. de déterminer les responsabilités des différents échelons hiérarchiques;
3. de constituer un document de travail pour les différents échelons de commandement et plus particulièrement, pour le personnel spécifiquement chargé de la sécurité;
4. de mettre à la disposition de tous les membres du cadre un document général de base.

L'IF 5 stipule que le Chef du Service Général de Renseignement et de Sécurité (SGR) est responsable :

"Dans le domaine de la sécurité militaire préventive :

- a) de la rédaction et de la diffusion des règlements, directives et normes pour assurer la sécurité militaire en ce qui concerne :
 - le personnel ;
 - l'information et le traitement de l'information ;
 - le matériel ;
 - les installations ;
 - les activités ;

- b) de l'avis concernant les Directives Complémentaires de Sécurité (DCS) établies par le Commandant du Commandement Territorial Interforces (CTI);
- c) de l'exécution des inspections de sécurité afin de contrôler l'application des règlements, directives et normes de sécurité dans l'ensemble des Forces Armées ;
- d) de l'exécution des enquêtes après des incidents de sécurité."

D'autre part, l'IF 5 détermine les responsabilités :

- des chefs des divisions et des services rattachés de l'Etat-Major général;
- des chefs d'Etat-major des différentes Forces ;
- du Commandant du Commandement Territorial Interforces ;
- des Commandants des échelons de commandement et territoriaux subordonnés ;
- de l'officier de sécurité et prévoit pour celui-ci en particulier :
 - de mettre au courant le Commandant des infractions, lacunes ou vulnérabilités liées à la sécurité, et de faire des propositions pour y remédier ;
 - d'exécuter une enquête de sécurité en cas d'infraction réelle ou probable contre la sécurité.

La sécurité est une responsabilité du Commandant. Ce principe est valable pour tous les échelons et pour chaque organisme militaire.

Pour aider le Commandant à exercer cette responsabilité, il désignera un officier, nommé officier de sécurité.

L'IF 5 définit enfin la responsabilité individuelle dans le domaine de la sécurité.

En effet, en dehors de la responsabilité du Commandement et des tâches spécifiques attribuées à l'officier de sécurité, il est indispensable que chaque membre de l'armée – quel que soit sa catégorie, son rang ou son grade –, assume sa responsabilité dans le domaine de la sécurité militaire.

Le règlement IF 5 parle de plusieurs zones, telles que :

une zone *classifiée* : zone dans laquelle se trouve des informations classifiées ;

une zone *protégée* : les zones classifiées, les locaux de garde, les dépôts de munitions et les magasins d'armes ;

une unité *protégée* : unité où se trouve des informations classifiées et où des activités classifiées sont effectuées pour lesquelles tout le personnel doit disposer au minimum d'une habilitation de sécurité du niveau le plus faible.

Enfin, on parle de "*zone particulièrement protégée*", bien que celle-ci ne soit pas définie dans le document précité, s'il s'agit de dépôt de munitions car ceux-ci présentent la particularité que leur accès est contrôlé et enregistré.

La procédure d'accès à ces zones est décrite dans différentes rubriques.

La rubrique 714 porte plus particulièrement sur la sécurité des dépôts de munitions et indique:

- "a. Les dépôts de munitions sont des "zones protégées particulières" qui doivent répondre aux normes de sécurité prévues dans le règlement IF 5bis.*
- b. L'accès doit en être strictement limité. Ceci fera l'objet de directives précises de l'autorité de sécurité hiérarchique.*
- c. Tous les visiteurs, inclus les détenteurs de cartes d'accès spéciales, seront inscrits dans un registre qui sera conservé pendant cinq ans."*

Remarquons à cet égard que le personnel, qui doit avoir accès à une zone classifiée ou à une unité protégée, doit disposer d'une habilitation de sécurité.

Pour le personnel qui doit avoir accès aux locaux de garde, aux dépôts de munitions et aux magasins d'armes ou à une zone particulièrement protégée, ce principe ne s'applique pas.

3.2. Les "Directives Complémentaires de Sécurité" (DCS)

Celles-ci comprennent les dispositions relatives à la sécurité militaire qui sont localement ou temporairement d'application et/ou portent seulement sur une partie des forces armées.

Ces directives sont établies par le Commandant du Commandement Territorial Interforces (CTI) en coordination avec les chefs d'Etat-major des forces , et diffusées après approbation de leur contenu par le chef de l'Etat-major, après avis du chef du SGR.

4. RESUME DE L'ENQUETE

4.1. Enoncé du problème

Le 23 septembre 1997, il a été constaté qu'un lot important de munitions avait été dérobé par effraction entre le 1^{er} juin 1997 et le 22 septembre 1997, au dépôt de munitions militaire de Houthulst au préjudice du Ministère de la Défense nationale.

Le dépôt de munitions militaire se trouve sur le territoire de la commune de Houthulst, en Flandre-Occidentale, et a été implanté au lieu-dit "Bos van Houthulst".

Différentes unités utilisent ce dépôt comme entrepôt pour leurs munitions.

Le Comité R et son Service d'enquêtes souhaitent, en l'espèce, savoir quelles étaient les compétences du SGR et si ce service avait effectué ses missions de manière efficace.

4.2. Enquête à la suite du vol

Le 4 septembre 1997, il a été constaté que certaines munitions manquaient dans un magasin.

Le commandant du dépôt a été informé de cette constatation.

A partir du 19 septembre 1997, une série d'autres disparitions de munitions a été constatée dans d'autres magasins.

A partir de cette date, le SGR/SMI a reçu à ce sujet des avis urgents et des rapports concis.

Le 23 septembre 1997, la gendarmerie locale a été informée de ces disparitions.

L'"Unité de Sécurité Interforces" (USI) locale a également entamé une enquête.

4.3. Les responsabilités pour la protection et la surveillance du dépôt de munitions

La protection et la surveillance de ces dépôts et magasins relèvent de la responsabilité de l'autorité militaire qui en a la gestion.

Cette responsabilité est exercée sous différents contrôles militaires.

Afin de tenir compte des circonstances locales concrètes, les consignes détaillées en la matière sont établies par l'autorité responsable locale, compte tenu des directives IF 5, IF 5bis et des dispositions du CTI.

L'application de ces consignes est contrôlée :

- par l'USI (Unité de Sécurité Interforces) pour la chaîne territoriale,
- par les inspections du commandement pour la chaîne hiérarchique,

Dans le cadre de ces contrôles, le SGR/SMI peut être sollicité pour intervenir comme conseiller.

4.4. Compétences du SGR en la matière

4.4.1. Généralités

Les compétences du SGR/SMI consistent à conseiller le commandement militaire responsable sur les mesures de protection recommandées, la vérification de leur exécution, la constatation dans ces circonstances de lacunes éventuelles, de la transmission des défaillances constatées au commandement militaire précité et la formulation des recommandations nécessaires pour y remédier.

Après la constatation des faits à Houthulst, l'officier de permanence du SGR/S a été informé par un avis urgent, conformément aux dispositions du règlement IF 5. C'est la règle lorsqu'un incident de sécurité survient dans un domaine militaire.

En fonction du lieu, de la nature et de l'importance de l'incident, l'on réagit de manière adaptée.

En cas d'incident dans un organisme/une unité militaire pour lequel l'"Unité de Sécurité Interforces" (USI) du "Commandement Territorial Interforces" (CTI) est compétente, l'enquête est réalisée en premier lieu par l'USI précitée.

Si la nature et l'importance de l'incident revêtent un caractère limité et local, le SGR/SMI consignera les résultats de l'enquête et les mesures prises en vue d'évaluations générales ultérieures.

C'est la procédure qui a été suivie après les faits commis à Houthulst.

Dans le cas où le résultat de l'enquête effectuée par l'USI ne satisfait pas, le SGR/SMI peut demander soit d'approfondir l'enquête, soit de lancer sa propre enquête.

4.4.2. Les contrôles effectués par le SGR/SMI

Principe général

Le SGR/SMI ne dispose pas du personnel et des moyens nécessaires pour effectuer des contrôles systématiques.

Cette section intervient comme conseiller du commandement concerné, lorsqu'elle y est invitée. Elle intervient également de sa propre initiative lors de la constatation de défaillances.

Le contenu et la manière dont un contrôle se déroule dépendent essentiellement des circonstances (contrôle sur demande ou à l'improviste, pendant ou en dehors des heures de service, complet ou partiel, etc...).

En principe, un rapport est établi après le contrôle pour confirmer le récit oral qui a été fait directement sur place.

Ce rapport est transmis à l'autorité qui a demandé les conseils ou, si le contrôle a été effectué d'initiative, à l'autorité responsable de la gestion.

La hiérarchie fonctionnelle (Etat-major de la Force armée) et la hiérarchie territoriale (Etat-major du Commandement Territorial Interforces) sont également informées.

Les mesures prises à la suite de ces rapports dépendent de la nature des défaillances constatées et des circonstances locales. Les autorités militaires compétentes doivent, en outre, tenir compte des moyens disponibles en matière de personnel, de matériel et de budget.

Contrôles exercés par le SGR/SMI au dépôt de munitions de Houthulst

Tout d'abord, il faut indiquer que le rapport confidentiel du 10 mars 1998 de l'Unité de Sécurité Interforces locale, établi à la suite du vol commis, fait mention de rapports établis depuis 1994.

Dans le cadre de la mise au point des normes d'infrastructure par l'Etat-major de la Force terrestre, le SGR/SMI a visité tous les grands dépôts de munitions régionaux et locaux en 1996 ou 1997. Le dépôt de munitions de Houthulst a fait l'objet d'une inspection le 13 février 1997.

Durant les inspections précitées, la situation de la sécurité de ces dépôts a été jugée insuffisante, car la réduction des effectifs du personnel de garde (à la suite de la suppression du service militaire) n'avait pas encore été compensée par des améliorations de la protection des infrastructures.

A la suite des visites effectuées par les différentes autorités compétentes et des constatations faites par le SGR/SMI, celui-ci a établi une note le 17 mars 1997 dans laquelle le SGR/SMI insistait sur les mesures à prendre d'urgence, et qui décrivait et diffusait les mesures recommandées aux diverses autorités compétentes.

Le 18 février 1998, un briefing a été organisé et des conclusions tirées avec toutes les parties qui ont participé aux différentes visites.

Se fondant sur les résultats de ce briefing, l'Etat-major général a publié ses options par une note du 7 avril 1998 au Chef d'Etat-major général de la Force terrestre.

Depuis 1993, de nouvelles normes ont été décrétées pour les magasins d'armes et de munitions, et elles ont été confirmées dans la nouvelle version du règlement IF5 Bis Partie 1 (en mai 1997).

Les normes sont respectées pour toutes les nouvelles constructions et sont progressivement appliquées à toutes les anciennes infrastructures. Une priorité plus élevée est accordée à cet égard à l'adaptation des magasins d'armes.

5. CONCLUSIONS

Le Comité R constate que les forces armées disposent d'abondantes directives de sécurité qui définissent les responsabilités et la compétence spécifiques à chaque échelon.

L'analyse de ces directives et d'autres documents mis à disposition montre que des fautes étaient commises depuis un certain temps déjà en matière de sécurité au dépôt de munitions de Houthulst.

Cela est notamment confirmé par le rapport confidentiel du 10 mars 1998 de l'Unité de Sécurité Interforces locale, établi à la suite du vol commis.

En ce qui concerne le SGR et le SGR/SMI, l'enquête n'a constaté aucun dysfonctionnement. Dans la note du SGR/SMI du 17 mars 1997, qui a été diffusée aux diverses autorités, les problèmes de sécurité qui se posaient en matière de dépôt de munitions ont été clairement soulignés et des propositions ont également été élaborées pour y remédier.

Bien que le SGR puisse formuler des recommandations au sujet des mesures de sécurité à prendre, il ne dispose cependant pas des moyens financiers ou matériels pour aider les organismes inspectés à améliorer les défaillances constatées.

Les autorités militaires compétentes doivent tenir compte des moyens disponibles en personnel, en matériel et en budget.

Du fait de la suppression du service militaire obligatoire et de la réorganisation des forces armées, des moyens importants ont été supprimés, ce qui ne facilite pas l'exécution de la tâche imposée.

Au niveau du SGR/SMI, aucune nouvelle directive n'a été établie étant donné que le strict respect des directives actuelles suffit pour prévenir de tels vols.

La Force armée concernée elle-même a dégagé des moyens pour améliorer les protections infrastructurelles.

La Sûreté de l'Etat n'a pas été informée des faits. Initialement, rien n'indiquait qu'il s'agissait d'autre chose que d'un vol ordinaire. Ce n'est que plus tard que l'on a constaté, sur la base de l'enquête judiciaire, l'implication d'un membre du personnel de l'unité et du club de motards " Hells Angels ".

L'échange d'informations entre le SGR et la Sûreté de l'Etat concernant la problématique de la sécurité en matière de dépôts de munitions et d'armes se déroule au sein du GMA (Groupe Mixte Antiterroriste) pour l'évaluation de la menace. Ce groupe réunit notamment des représentants des deux services précités.

6. RECOMMANDATIONS

Il est clairement apparu de l'enquête menée que des problèmes de communication surviennent souvent en raison de la procédure assez lourde utilisée au sein des forces armées.

Le Comité R recommande donc que le SGR, dans la mesure du possible :

- vérifie si les autorités compétentes en la matière ont été correctement informées à l'aide des pièces qui lui sont transmises par les différentes unités;

- vérifie, à intervalles réguliers, au sein de ces autorités si les défaillances signalées ont été résolues.

De plus, il serait souhaitable que les règlements IF 5 soient adaptés afin de prévoir une enquête de sécurité minimale en ce qui concerne les membres du personnel (militaires ou civils) qui sont appelés à effectuer des missions dans les zones particulièrement protégées.

La possibilité d'une collaboration avec les services de police locaux devrait être envisagée. Deux solutions semblent à prendre en considération à cet égard.

1. au niveau local : cette collaboration pourrait être réglée par le commandant de quartier, mais cela dépendra de sa relation personnelle avec les services de police locaux.
2. sur le plan général : une telle collaboration pourrait être éventuellement réglée au moyen de protocoles d'accords entre les autorités compétentes.

D. LES PLAINTES

CHAPITRE 1 : ENQUETE DE CONTROLE RELATIVE A LA PLAINTE DE MONSIEUR X

1. PROCÉDURE

Le 29 septembre 1998, Monsieur X a déposé une plainte verbale auprès du Service d'enquêtes du Comité R, à l'encontre de la Sûreté de l'Etat au motif que celle-ci aurait fourni à la Chambre des Représentants des renseignements défavorables et erronés à l'occasion de sa demande de naturalisation.

Cette demande de l'intéressé a effectivement fait l'objet d'une décision de rejet au début de 1998 motivée de la manière suivante : *"(...) et tenu compte des éléments négatifs de votre dossier, la Chambre des Représentants a décidé de rejeter cette demande de naturalisation étant donné que votre séjour en Belgique est limité à la durée de vos études"*.

Monsieur X avait d'abord entamé une demande de changement de son statut d'étudiant auprès du Ministère de l'Intérieur. Cette demande lui fut refusée fin 1997.

Insatisfait du rejet de sa demande de naturalisation au motif que son séjour en Belgique était limité à la durée de ses études, Monsieur X prit contact avec le Président de la Commission des Naturalisations. Celui-ci lui précisa par sa lettre du 24 mars 1998 que la décision prise au sein de la Commission l'avait été sur base d'un rapport circonstancié de la Sûreté de l'Etat.

Monsieur X conteste ces informations.

Le plaignant a réagi en écrivant en avril 1998 à l'Administrateur général de la Sûreté de l'Etat afin de faire rectifier les éléments contenus dans son dossier. Par lettre de juin 1998 l'Administrateur général répondit à l'avocat du plaignant : *" (...) la Sûreté de l'Etat ne souhaite pas donner suite à votre demande d'entretien et confirme son avis rendu dans le cadre de la demande de naturalisation introduite par votre client"*. Par courrier de début juillet 1998 l'Administrateur général fit savoir à l'avocat du plaignant qu'il ne lui semblait pas opportun de poursuivre un échange de courrier en ce qui concerne le cas de Monsieur X.

Par la plainte qu'il adresse au Comité R, Monsieur X espère faire revoir l'avis donné par la Sûreté de l'Etat lors de sa demande d'octroi de la nationalité belge afin qu'il puisse, le cas échéant, introduire une nouvelle demande de naturalisation.

Lors de sa réunion du 13 octobre 1998, le Comité R a décidé d'ouvrir une enquête de contrôle intitulée : *"Plainte d'un particulier à propos d'une éventuelle intervention de la Sûreté de l'Etat dans une procédure de naturalisation"*.

Deux membres du Comité R ont été chargés de mener cette enquête, et de tenir le Comité R régulièrement informé de son déroulement.

Le 13 octobre 1998, une apostille a été adressée au chef du Service d'enquêtes, le priant de consulter le dossier éventuel du plaignant au sein de la Sûreté de l'Etat et de faire la synthèse des éléments figurant dans ce dossier .

Conformément à l'article 46 § 3 du règlement d'ordre intérieur, les présidents de la Chambre et du Sénat ont été avertis de l'ouverture de cette enquête par lettre du 15 octobre 1998.

Le 16 octobre 1998, le chef du Service d'enquêtes a averti le Ministre de la Justice de l'ouverture de cette enquête conformément à l'article 43 § 1 de la loi organique du contrôle des services de police et de renseignements.

Le présent rapport a été approuvé par le Comité R le 10 décembre 1998.

2. NORMES APPLICABLES À LA PROBLÉMATIQUE

L'article 21 § 3 et 4 de la loi du 28 juin 1984 relative à certains aspects de la condition des étrangers et instituant le code de la nationalité belge, modifiée par la loi du 13 avril 1995, stipule :

“ § 3. La Chambre des Représentants transmet la demande de naturalisation au parquet près le tribunal de première instance de la résidence principale du demandeur, pour avis à fournir dans un délai de 4 mois.”

“ § 4. La chambre des représentants peut demander, à toutes les autorités et notamment au parquet près le tribunal de première instance de la résidence principale du demandeur, de procéder à une enquête relative aux critères prévus à l'article 19 et aux conditions et circonstances prévues à l'article 15 § 2, ainsi qu'à tout élément sur lequel la Chambre des représentants souhaite être informé.” (...)

L'article 15 § 2 rencontre le critère relatif à la volonté d'intégration tandis que l'article 19 énonce les conditions formelles requises pour introduire sa demande (âge, résidence en Belgique, etc...).

L'exposé des motifs de la proposition de loi ⁽¹⁾ énonce : *“le substitut demande alors l'avis de la Sûreté de l'Etat et celui de l'Office des étrangers.”*

L'obtention de la nationalité belge par la voie de la naturalisation n'est pas un droit , mais résulte de l'exercice d'un pouvoir souverain reconnu au pouvoir législatif, principe rappelé par la Cour d'Arbitrage ⁽²⁾.

(1) Doc parl. Sénat de Belgique- session 1994-1995/1247 - 2 p. 5

(2) Cour d'Arbitrage - arrêt n° 75/98 - 24/06/1998 .

3. SYNTHÈSE DE L'ENQUÊTE

Le Service d'enquêtes du Comité R s'est rendu à la Sûreté de l'Etat pour consulter le dossier du plaignant.

L'étude de ce dossier établit que la Commission des Naturalisations de la Chambre des Représentants s'est renseignée auprès de la Sûreté de l'Etat .

La réponse de la Sûreté de l'Etat dresse l'inventaire des activités de l'intéressé exercées publiquement .

La Sûreté de l'Etat n'a pas pris position; son rôle s'est limité à documenter la Chambre des Représentants .

Les activités de Monsieur X n'ont plus attiré l'attention de la Sûreté de l'Etat depuis 1991.

4. CONCLUSIONS

Dans le cadre de sa mission de contrôle , le Comité R n'a pas relevé d'indices permettant d'établir que les droits que la Constitution et les lois belges confèrent au plaignant ont été violés.

CHAPITRE 2 : ENQUÊTE DE CONTRÔLE SUR PLAINTE DE MONSIEUR Y

1. PROCÉDURE

Par lettre du 12 juin 1998, le conseil de Monsieur Y, a déposé plainte entre les mains de la présidente du Comité R, à l'encontre de la Sûreté de l'Etat pour comportement abusif et non fondé à l'égard de son client à l'occasion de la demande de ce dernier dans le cadre d'une procédure de naturalisation.

L'intéressé avait fait l'objet d'une décision de rejet de demande de naturalisation en 1996 pour les raisons suivantes : *“manque d'intégration qui se traduit par des activités orientées vers son pays d'origine”*.

Le conseil de Monsieur Y mettait cette motivation en rapport avec l'avis rendu par l'Office des étrangers, de 1995, concernant la dérogation à la nationalité belge que Monsieur Y avait demandé pour l'exercice de la profession de professeur de religion islamique. Cet avis est défavorable pour “raison de sûreté publique” en janvier 1995 pour devenir favorable en avril 1995.

L'objectif de la plainte avait pour but de connaître les informations de la Sûreté de l'Etat qui justifieraient que l'on puisse invoquer la raison de sûreté publique notamment pour refuser à Monsieur Y l'octroi de la nationalité belge afin qu'il puisse le cas échéant transmettre une réponse circonstanciée à la Commission des Naturalisations de la Chambre des Représentants.

Lors de sa réunion du 9 juillet 1998, le Comité R a décidé d'ouvrir une enquête de contrôle intitulée : *“Plainte d'un particulier à propos d'une éventuelle intervention de la Sûreté de l'Etat dans une procédure de naturalisation”*.

Deux membres du Comité R ont été chargés de mener cette enquête, et de tenir le Comité R régulièrement informé de son déroulement.

Conformément à l'article 46 § 3 du règlement d'ordre intérieur, les présidents de la Chambre et du Sénat ont été avertis de l'ouverture de cette enquête par lettre du 14 juillet 1998.

A la même date, un accusé de réception a été envoyé au conseil du plaignant. Cette lettre mentionnait que l'avocat du plaignant serait avisé, dès la clôture de l'enquête, de la décision qui sera arrêtée par le Comité R.

Le 18 août 1998, une apostille a été adressée au chef du Service d'enquêtes, le priant de consulter le dossier du plaignant à l'Office des étrangers, de vérifier si la Sûreté de l'Etat est intervenue dans la procédure de naturalisation du plaignant et dans l'hypothèse positive de quelle manière et pour quelles raisons.

Le 19 août 1998, le chef du Service d'enquêtes a averti le Ministre de la Justice de l'ouverture de cette enquête conformément à l'article 43 § 1 de la loi organique de contrôle des services de police et de renseignements.

Le présent rapport a été approuvé par le Comité R le 19 novembre 1998.

2. NORMES APPLICABLES À LA PROBLÉMATIQUE

L'article 21 § 3 et 4 de la loi du 28 juin 1984 relative à certains aspects de la condition des étrangers et instituant le code de la nationalité belge, modifiée par la loi du 13 avril 1995, stipule

“ § 3. La Chambre des Représentants transmet la demande de naturalisation au parquet près le tribunal de première instance de la résidence principale du demandeur, pour avis à fournir dans un délai de 4 mois.”

“ § 4. La chambre des représentants peut demander, à toutes les autorités et notamment au parquet près le tribunal de première instance de la résidence principale du demandeur, de procéder à une enquête relative aux critères prévus à l'article 19 et aux conditions et circonstances prévues à l'article 15 § 2, ainsi qu'à tout élément sur lequel la Chambre des représentants souhaite être informé.” (...)

L'article 15 § 2 rencontre le critère relatif à la volonté d'intégration tandis que l'article 19 énonce les conditions formelles requises pour introduire sa demande (âge, résidence en Belgique, etc...).

L'exposé des motifs de la proposition de loi ⁽¹⁾ énonce : *“le substitut demande alors l'avis de la Sûreté de l'Etat et celui de l'Office des étrangers. En application des circulaires du 22 septembre et 15 octobre 1993 du ministre de la Justice, si la réponse de l'Office des étrangers ne parvient pas dans un délai de deux mois au parquet, l'avis est présumé favorable et la procédure suit son cours.”*

Le ministère de la Justice a transmis au Service d'enquêtes la circulaire ministérielle du 6 août 1984. Cette circulaire stipule en sa page 4 : *“Encore une fois, ce qui importe est l'intégration et non l'assimilation : il s'agit, non pas de demander à l'étranger d'être en tout semblable aux belges de naissance et de perdre tout caractère distinctif rappelant ses origines, mais d'exiger qu'il manifeste par son comportement, et non seulement par ses déclarations, qu'il désire vivre avec les belges et en harmonie avec eux. A cet égard, la circonstance qu'un immigré vit exclusivement en milieu étranger peut être considérée, parmi d'autres, comme significative.*

(1) Doc parl. Sénat de Belgique- session 1994-1995/ 1247 - 2 p. 5

Non qu'elle soit répréhensible; ce peut être une forme de fidélité ou une conséquence du fait que certains étrangers ne sont pas bien accueillis. Mais, quelle que soit la cause, l'absence de contacts avec les Belges rend l'intégration difficile. (...)

Cette circulaire qui date d'avant l'entrée en vigueur de la loi du 13 avril 1995, n'a pas été modifiée, ni abrogée. Elle confirme la circulaire du Procureur général datée du 15 novembre 1947.

3. SYNTHÈSE DE L'ENQUÊTE

Le Comité R a interrogé le président de la Commission d'accès aux documents administratifs et le président de la Commission de la protection de la vie privée afin de savoir si le plaignant avait également porté à leur connaissance sa problématique de refus de naturalisation.

Par lettre du 15 octobre 1998, le président de la Commission d'accès aux documents administratifs a répondu par la négative.

Par lettre du 12 novembre 1998, le président de la Commission de la protection de la vie privée a répondu que le plaignant n'avait pas soumis le problème de refus de sa demande de naturalisation à la Commission.

Le Service d'enquêtes du Comité R s'est rendu à la Sûreté de l'Etat et à l'Office des étrangers pour consulter le dossier du plaignant.

Il résulte de l'étude de ce dossier que la Sûreté de l'Etat a transmis au parquet de Bruxelles des informations, sans prendre position. Ces informations décrivent les activités du plaignant, exercées publiquement. La Sûreté de l'Etat a tiré ses renseignements de l'analyse des sources que l'on peut qualifier d'ouvertes, sans émettre le moindre avis.

Le parquet de Bruxelles en a déduit le défaut de volonté d'intégration dans le chef du plaignant et a fait connaître son avis à la Chambre des Représentants, qui a en 1996 pris la décision de rejet de demande de naturalisation eu égard à *"sa volonté (du plaignant) d'intégration insuffisante"*.

4. CONCLUSIONS

Le Comité R n'est pas habilité à donner au plaignant accès au dossier détenu par la Sûreté de l'Etat.

Pour le surplus, dans le cadre de sa mission de contrôle, le Comité R n'a pas relevé d'indices permettant d'établir que les droits que la Constitution et les lois belges confèrent au plaignant ont été violés.

CHAPITRE 3 : ENQUETE DE CONTROLE CONSECUTIVE A LA PLAINTE DEPOSEE PAR MONSIEUR Z

1. PROCEDURE

Par lettre du 21 janvier 1999, Monsieur Z a fait parvenir une plainte au chef du Service d'enquêtes du Comité R.

Dans cette plainte, Monsieur Z mentionne plusieurs faits qui ne sont pas de la compétence du Comité R. Toutefois, il veut connaître les raisons pour lesquelles un certificat de sécurité "Secret Otan" lui a été refusé.

La plainte a été transmise au Comité R le 27 janvier 1999. Par son apostille du 4 février 1999, le Comité R a prié le chef du Service d'enquêtes de procéder à l'audition du plaignant.

Le Comité R a reçu le rapport d'audition le 18 février 1999 et au cours de sa réunion du 25 février 1999, il a décidé d'ouvrir une enquête de contrôle consécutive à la plainte déposée par Monsieur Z au sujet du refus du SGR de délivrer un certificat de sécurité.

Le Comité R a chargé l'un de ses membres de suivre l'enquête, de la superviser et d'en faire régulièrement rapport.

Par apostille du 25 février 1999, le Comité R a chargé le chef du Service d'enquêtes de vérifier s'il existait bien un dossier, au SGR, au nom de Monsieur Z et, dans l'affirmative, d'en prendre connaissance.

Conformément à l'article 46, alinéa 3 du règlement d'ordre intérieur du Comité R, les Présidents de la Chambre des Représentants et du Sénat ont été informés de l'ouverture de l'enquête par lettre du 26 février 1999.

Conformément à l'article 43, alinéa 1 de la loi organique du 18 juillet 1991 sur le contrôle des services de police et de renseignements, le chef du Service d'enquêtes a informé le Ministre de la Défense nationale, à la date du 2 mars 1999, qu'une enquête était effectuée

2. RÉSUMÉ DE L'ENQUÊTE

2.1. Audition du plaignant

Il est ressorti de son audition que le plaignant a été engagé par une firme en novembre 1997 et qu'il a été licencié en juin 1998 pour cause de réorganisation de l'entreprise. Monsieur Z a ajouté que la firme qui l'employait, aurait souhaité exécuter des travaux pour le compte de l'OTAN.

Monsieur Z n'est pas certain qu'une demande de certificat de sécurité a été introduite à son nom, bien qu'il déclare avoir rempli des documents semblables à ceux qui sont exigés pour l'octroi d'un tel certificat.

Monsieur Z a déposé plainte auprès du chef du Service d'enquêtes aux fins de savoir, entre autres, si la firme avait demandé un certificat de sécurité pour lui et, dans l'affirmative, les motifs pour lesquels ce certificat de sécurité ne lui a pas été accordé.

2.2. Examen du dossier conservé au SGR

Le Service d'enquêtes a pu prendre connaissance du dossier que le SGR a ouvert sur l'intéressé.

Un document daté de novembre 1997 renvoie à une demande de certificat de sécurité du niveau "Secret OTAN" introduite au nom de Monsieur Z par l'officier de sécurité de la firme. Il ressort des pièces du dossier qu'en novembre 1997, Monsieur Z a rempli et signé un formulaire de demande d'une habilitation de sécurité du degré secret. L'officier de sécurité de la firme a envoyé ledit formulaire au SGR en novembre de la même année.

L'enquête de sécurité menée dans ce contexte a été effectuée par le SGR/Gd sur base des données fournies par Monsieur Z.

Il est ressorti de l'enquête que l'autorité compétente a décidé à l'unanimité de ne pas lui faire confiance. C'est pour ce motif que le certificat de sécurité lui a été refusé.

L'autorité militaire responsable a notifié cette décision à la firme par une lettre de février 1998. Le motif qui conduit au refus d'un certificat de sécurité ne sera et ne pourra jamais être communiqué.

3. CONSTATATIONS

Il est clairement ressorti de l'enquête menée par le Service d'enquêtes qu'en sa qualité d'employé de la firme, le plaignant a effectivement rempli un formulaire visant à obtenir un certificat de sécurité du degré secret. Il ressort des déclarations du plaignant qu'il savait pertinemment bien avoir rempli un tel formulaire, étant donné qu'il avait déjà été confronté à des demandes semblables dans le passé. Aussi est-il surprenant que Monsieur Z ait déposé plainte pour savoir si la firme avait demandé, pour lui, un certificat de sécurité.

La procédure suivie par la firme a été parfaitement régulière.

La sécurité au sein de l'OTAN est en tout cas réglée par le document C-M (55) 15 (définitif). En exécution des règlements de sécurité de l'OTAN, chaque Etat membre a créé un organisme national de sécurité responsable de l'application des règlements, à savoir l'Autorité de sécurité nationale (ASN).

L'ASN a délégué ses compétences au chef du Service général de la sécurité et du renseignement (SGR), en ce qui concerne les aspects de la sécurité relatifs au Ministère de la Défense nationale et aux activités industrielles pour lesquelles l'accès aux informations classifiées doit être réglementé.

La plainte de Monsieur Z mentionne le fait que la firme visait un contrat avec l'OTAN. En l'occurrence, l'autorité compétente auprès de laquelle il fallait introduire la demande de certificat de sécurité était bien le SGR/SMI.

Par une lettre de février 1998, le responsable de l'autorité militaire a informé la firme que le certificat de sécurité n'avait pas été accordé à Monsieur Z.

4. CONCLUSIONS

Le Comité R estime que le SGR n'a en aucune façon illégitimement et sans justification porté atteinte aux droits et libertés du plaignant.

Le déroulement d'une enquête de sécurité et la délivrance d'un tel certificat sont aujourd'hui réglés par la loi du 11 décembre 1998 *relative à la classification et aux habilitations de sécurité*.

L'article 29 de cette loi dispose : "*Le Roi détermine la date d'entrée en vigueur des dispositions de la présente loi*".

Aucun arrêté d'exécution n'est intervenu à ce jour.

La loi du 11 décembre 1998 *portant création d'un organe de recours en matière d'habilitations de sécurité*, prévoit une procédure de recours pour les intéressés auxquels on a refusé ou retiré l'habilitation de sécurité.

Le Comité R est saisi du recours. Ici aussi, aucun arrêté d'exécution n'est encore intervenu.

Le Comité R espère que les deux lois précitées entreront en vigueur le plus vite possible.

E. SUIVI DES ENQUETES DES ANNEES PRECEDENTES

CHAPITRE 1 : ECHANGE DE VUES ENTRE LE COMITÉ PERMANENT R ET LES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ À LA SUITE D'UNE ENQUÊTE DE CONTRÔLE CONCERNANT LES INFORMATEURS DE LA SÛRETÉ DE L'ETAT ET DU SGR.

Dans son rapport d'activités de 1997, le Comité R a publié les résultats de l'enquête de contrôle concernant les informateurs utilisés par la Sûreté de l'Etat et le SGR.⁽¹⁾

Dans sa conclusion générale le Comité R soulignait *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. A l'avenir cette matière continuera à être traitée sous la forme de "case study".*

Par courrier du 1^{er} septembre 1997, le Ministre de la Justice a fait savoir au Comité R que la Sûreté de l'Etat avait mis sur pied un groupe de travail pour étudier la problématique des informateurs. Il signalait également que les résultats en seraient communiqués au Comité R.

Ce dernier avait proposé aux ministres compétents d'organiser un échange de vues en la matière. Par lettre du 6 novembre 1997, les ministres de la Justice et de la Défense nationale ont fait savoir à la présidente du Comité R qu'ils n'avaient pas d'objection à ce qu'un échange de vues soit organisé entre le Comité R, la Sûreté de l'Etat et le SGR.

Le 21 janvier 1998, le chef du SGR a porté à la connaissance de la présidente du Comité R que son service désirait participer aux discussions concernant l'élaboration d'une réglementation relative aux informateurs des services de renseignement. En même temps, il faisait part de diverses considérations dont il faudrait tenir compte lors des travaux.

Dans le courant du mois de janvier 1998, le Comité R a transmis à la Sûreté de l'Etat ainsi qu'au SGR, un certain nombre de directives non classifiées de services de renseignement étrangers ayant pour sujet la question des informateurs. Le but était de permettre à nos services de réfléchir sur ces textes en vue d'une future discussion avec le Comité R.

Le 25 septembre 1998, la présidente du Comité R rappelait au SGR et à la Sûreté de l'Etat l'échange de vues projeté, tout en soulignant que la documentation avait déjà été communiquée en janvier 1998.

(1) Rapport d'activités 1997, deuxième partie, B, Chapitre 1, p. 134 et suivantes.

Le 3 novembre 1998, un entretien réunissait le Comité R et le Chef du SGR accompagné du chef de la section SGR/IH et du conseiller juridique du SGR.

Le 25 novembre 1998, les mêmes personnes se rencontraient à nouveau avec cette fois le chef de la section du SGR/CI.

Le 2 février 1999, l'Administrateur général de la Sûreté de l'Etat eut un entretien avec le Comité R.

Durant ces différentes réunions, les recommandations formulées par le Comité R dans son rapport de 1997 furent discutées. C'est avec une très grande attention que furent abordées les questions de savoir ce qui serait réglé par des dispositions légales et ce qui ferait uniquement l'objet de directives classifiées et non classifiées. De surcroît, l'importance des principes de subsidiarité et de proportionnalité dans le cadre de l'utilisation d'informateurs a été mise en exergue.

Le Comité R a porté à la connaissance des différents services certains articles du projet de loi néerlandais concernant les services de renseignement et de sécurité. La matière des informateurs y est en effet spécifiquement réglementée.

Tous les participants aux différentes réunions partageaient sans réserve la même opinion sur la nécessité de s'entendre sur le contenu du mot "informateur". Pour certains, il s'agit d'une source, pour d'autres d'un agent, et de plus en Belgique il n'existe aucune définition légale de ce concept.

Après ces différentes rencontres, il est également apparu très clairement qu'il fallait tenir compte de la spécificité des divers services lors de la rédaction des directives.

Le Comité R considérait comme très positif le fait que tous les services soient disposés à mettre sur pied un groupe de travail composé de collaborateurs du SGR/S, SGR/CI, de la Sûreté de l'Etat et d'un ou plusieurs membres du Comité R, afin d'étudier comment cette matière pourrait être réglementée.

Par courrier du 30 mars 1999, le Chef du SGR transmettait les nouvelles directives concernant les informateurs au Comité R dans le but de participer à ce groupe de travail.

Le Comité R compte commencer les travaux de ce groupe dans les prochains mois, en tenant compte de la disponibilité des services qui ont à faire face à des missions multiples suite à l'entrée en vigueur le 1^{er} février 1999, de la loi organique des services de renseignement et de sécurité.

CHAPITRE 2 : RAPPORT RELATIF A L'ECHANGE DE VUES ENTRE LE SGR ET UN MEMBRE DU COMITE R CONCERNANT LA DESTRUCTION DE DOCUMENTS PAR LE SGR

Dans son rapport annuel de 1996, le Comité R a publié l'enquête de contrôle relative à la destruction de documents de la Sûreté de l'Etat et du SGR.

La destruction de documents et/ou de dossiers par les services de sécurité et de renseignements est une matière importante pour laquelle il faut tenir compte :

- de la protection des droits, en particulier le droit à la vie privée du citoyen;
- de l'intérêt de la recherche historique;
- de la possibilité de pouvoir vérifier la politique menée par les services de sécurité et de renseignements dans la collecte de données à caractère personnel, afin de pouvoir suivre l'évolution de la jurisprudence des services.

Pour le traitement de cette problématique, il faut tenir compte de diverses lois :

- 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 l'article 5 sur le principe de finalité);
- la loi du 11 avril 1994 relative à la publicité de l'administration;
- la loi du 24 juin 1955 relative aux archives;
- l'arrêté royal du 12 décembre 1957 concernant l'exécution de la loi du 24 juin 1955 relative aux archives.

A la suite de cette enquête de contrôle, le Comité R a formulé plusieurs recommandations.

Le Comité R a constaté que tant la Sûreté de l'Etat que le SGR ont consenti des efforts sérieux pour définir une procédure en matière de sélection et de destruction de dossiers.

Néanmoins, le Comité R a regretté que les services précités ne se soient aucunement concertés en vue de parvenir à des critères de sélection conjoints afin de mener une même politique de destruction.

En ce qui concerne le SGR, le Comité R estimait :

- que vu sa responsabilité politique, les critères de sélection doivent être préalablement approuvés par le ministre de la Défense nationale;
- que plusieurs dossiers doivent être conservés, par échantillonnage, en vue de vérifier la politique menée par le service concernant la collecte de données à caractère personnel. Cela est également nécessaire pour permettre au Comité R d'effectuer éventuellement un contrôle "a posteriori";
- que la destruction de dossiers individuels de personnes qui font partie de groupements suivis, en se basant uniquement sur le fait que ces personnes ont atteint "l'âge de 70 ans", n'était pas indiquée. Dans l'attente d'autres critères et/ou de critères complémentaires éventuels, le Comité R a proposé que dans une première phase ces dossiers soient sélectionnés et conservés dans un fichier distinct;
- que les Archives Générales du Royaume doivent être consultées pour la destruction de dossiers;
- qu'il serait également souhaitable de recueillir l'avis de la Commission de la protection de la vie privée.

Le Comité R a enfin proposé que les deux services agissent de la même manière, à savoir en trois phases :

1° tout d'abord procéder à la sélection;

2° conserver pendant un certain temps les dossiers sélectionnés, notamment pour évaluer les critères de sélection;

3° procéder à la destruction effective.

Après finalisation de chaque phase, il serait souhaitable que les services fassent un rapport à ce sujet au Comité R pour lui permettre d'accomplir sa mission légale.

Le 4 décembre 1998, la présidente du Comité R a adressé une lettre au chef du SGR en lui demandant si le SGR avait déjà commencé la procédure de destruction et, dans l'affirmative, s'il avait été tenu compte des recommandations formulées en la matière par le Comité R.

D'autre part, il était demandé si une concertation était intervenue avec la Sûreté de l'Etat concernant la procédure à suivre.

Par un courrier du 24 décembre 1998, le chef du SGR a fait savoir au Comité R qu'une épuration (uitzuivering) complète et correcte des dossiers existants se heurtait à plusieurs difficultés.

Un premier problème résidait dans le manque de moyens en personnel et en matériel pour effectuer ce travail.

Un deuxième obstacle, du point de vue du Chef du SGR, portait sur la législation et la réglementation qui rendent la tâche très difficile au service en matière de détermination de critères incontestables de destruction.

D'autre part, il a été signalé au Comité R que, vu la nécessité de procéder à une épuration du fichier de dossiers existants, une étude interne avait été entamée pour décrire avec précision tous les aspects de la problématique posée et faire une évaluation précise des moyens (humains, matériels...) qui seraient nécessaires pour traiter correctement ces aspects.

Dans une deuxième phase, une méthode de travail serait définie pour permettre une épuration effective des dossiers.

Enfin, ce courrier indiquait que l'on espérait réaliser la première phase de l'étude pour la fin février 1999.

Il a également été fait référence au fait qu'une concertation orale est intervenue dans cette problématique avec la Sûreté de l'Etat en octobre 1996 sur les procédures à suivre.

Par un courrier du 24 février 1999, le Comité R a fait savoir au Chef du SGR qu'il constatait que ce service était, dans la situation actuelle, dans l'impossibilité de procéder à l'épuration et à la destruction de ses documents.

Le Comité R a également insisté sur le fait qu'il faudrait reprendre la concertation avec la Sûreté de l'Etat.

A la suite de ce courrier, le Chef du SGR a proposé qu'un échange de vues intervienne entre le SGR et le Comité R.

Cette réunion s'est déroulée le 2 avril 1999 en présence des personnes suivantes :

le Général Simons, Chef du SGR ; le Général Michaux ; le Colonel Schrijvers (A/SGR) ; le Colonel Ghenne (Chef du SGR/S) ; le Major Decamps (Chef de cabinet) ; M. Bertrem, Commissaire principal de première classe (SGR/J) et Mme Danielle Cailloux (membre du Comité R).

Le SGR a expliqué la problématique relative à la destruction de documents.

Selon le SGR, celle-ci est de deux ordres :

1. l'importance du fichier - à savoir 500.000 dossiers -, en précisant que 75% des données concernaient des personnes pour lesquelles une enquête de sécurité avait été effectuée dans le cadre de la délivrance d'un certificat de sécurité. Pour épurer ces dossiers, cinq personnes qualifiées seraient nécessaires durant au moins 5 ans.

Le problème est alors de trouver le personnel disponible pour cette tâche compte tenu d'une part, du développement de la capacité opérationnelle du SGR qui se trouve dans une phase décisive et d'autre part, de l'effort actuel pour traduire en termes opérationnels les missions imposées au SGR par la législation récente - aussi bien dans le domaine du renseignement que de la sécurité.

2. le domaine législatif et réglementaire : à cet égard, le SGR met l'accent sur la réglementation juridique actuelle et en projet et sur la difficulté de fixer des critères d'épuration incontestables.

Le point de vue du Comité R a été explicité. L'attention a été attirée sur la législation en vigueur et surtout sur la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Bien que certains articles de cette loi ne s'appliquent pas au traitement de données à caractère personnel nécessaires à l'exécution des missions des services de sécurité et de renseignements, il faut néanmoins tenir compte de l'article 5 qui s'applique bien aux services précités et qui stipule ce qui suit :

“Les données à caractère personnel ne peuvent faire l'objet d'un traitement que pour des finalités déterminées et légitimes et ne peuvent pas être utilisées de manière incompatible avec ces finalités; elles doivent être adéquates, pertinentes et non excessives par rapport à ces finalités.”

Il faut également tenir compte de l'article 39 § 3, qui prévoit qu'une infraction à l'article 5 est punie d'une amende de 100 BEF à 100.000 BEF et enfin de l'article 13, qui prévoit un accès indirect du citoyen, par l'intermédiaire de la Commission de la protection de la vie privée, au traitement des données, gérées par les services de sécurité et de renseignements.

Le fait que les services de sécurité disposent à présent d'une législation applicable depuis le 1^{er} février 1999, indiquant clairement qu'un arrêté royal déterminera la durée de conservation des données à caractère personnel ainsi que la procédure de destruction à suivre, ne dispense pas ces services des obligations imposées par la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Il est donc d'une importance capitale que le SGR commence également la procédure de sélection et de destruction des documents qui ne répondent plus au principe de finalité.

Pendant la discussion, les participants ont reconnu qu'un travail déjà très important avait été réalisé en matière de définition des critères d'épuration, compte tenu des propositions formulées en son temps par le SGR et retenues pour l'essentiel dans ses recommandations par le Comité R.

Le principe de prélever des dossiers à titre d'échantillon afin de vérifier la politique menée par le service de renseignements par rapport à la collecte de données à caractère personnel, a été discuté.

Parmi les dossiers entrant en considération pour leur destruction, un nombre suffisamment important de ceux-ci seront extraits afin de conserver des informations sur les méthodes de travail du service.

Bien que le Ministère de la Défense nationale soit dispensé de l'obligation de déposer ses archives aux Archives du Royaume, il n'empêche qu'il ne peut détruire aucun document sans l'accord de cette institution.

Selon le Comité R, il suffit de soumettre les critères de sélection aux Archives Générales du Royaume pour obtenir une autorisation globale de procéder à la destruction de documents conformément aux critères proposés.

Il est clairement apparu de cette concertation que le problème auquel le SGR est confronté pour lancer la procédure concernant la sélection et l'épuration de dossiers, est un manque de personnel.

En effet, il faut disposer d'une faculté de discernement pour appliquer les critères de sélection et cette tâche devra être effectuée dans la mesure du possible par du personnel qualifié.

En 1995 déjà, l'autorisation a été donnée à la Sûreté de l'Etat d'engager du personnel contractuel.

L'Administrateur général de la Sûreté de l'Etat a fait savoir au Comité R en novembre 1998 que la première phase (à savoir, la phase de sélection) était en cours et ajoutait, en mars 1999, que cette phase durerait certainement encore deux ans.

Vu l'évolution actuelle de la législation qui déterminera à l'avenir beaucoup plus clairement combien de temps les services de sécurité et de renseignements peuvent conserver des données à caractère personnel, il semble fortement recommandé que le SGR commence également l'épuration de ses anciens dossiers.

Cette obligation résulte d'ailleurs clairement de la loi du 8 décembre 1992 relative à la protection de la vie privée.

De plus, il conviendrait que les deux services ne se satisfassent plus simplement d'une concertation dans cette matière, mais que les différentes phases puissent être effectuées en même temps dans les deux services, dans la mesure du possible.

Le Comité R se permet donc d'insister pour que le SGR puisse disposer de personnel qualifié suffisant afin de pouvoir accomplir cette tâche non négligeable et prévue par la loi.

Par courrier du 23 juillet 1999, le SGR a fait savoir que l'Administrateur général de la Sûreté de l'Etat et le Chef du SGR ont convenu que le Chef du service juridique du SGR (SGR/J) veillerait à s'informer dans le courant du mois de septembre de la manière dont concrètement le problème relatif à la destruction des archives est traité par la Sûreté de l'Etat.

TITRE III : CONTACTS DU COMITE

CHAPITRE 1 : Journées d'étude

15 septembre 1998 : Techniques de protection pour le 21ème siècle

2 octobre 1998 : Les droits de l'homme sur Internet

Professeur Dumortier : Signature électronique : aspects juridiques

Le Professeur Jos Dumortier, professeur à la Faculté de Droit de la K.U. Leuven, part de l'hypothèse selon laquelle toute forme de signature est admise entre deux parties, à l'exclusion de certaines transactions pour lesquelles des exigences de forme sont imposées. En cas de litige, il incombera au juge de trancher avec, en règle générale, acceptation de tous les moyens de preuve.

L'orateur indique que deux courants coexistent au niveau européen pour régulariser le problème de la reconnaissance juridique de la signature électronique.

En Italie, la loi (Legge 15 marzo 1997 - nE 59) confère une reconnaissance juridique à la signature électronique, en marge de la signature traditionnelle, à la condition que la signature électronique réponde à diverses conditions. La reconnaissance s'applique à toute fin légale aux signatures des pouvoirs publics et des particuliers. Le législateur s'attelle encore à l'heure actuelle à la description technique des conditions auxquelles la signature doit satisfaire. Ces conditions ont pour l'essentiel trait à l'utilisation de la signature numérique, c'est-à-dire à une signature électronique reposant sur l'utilisation d'une cryptographie à clé publique. La mise en oeuvre de cette reconnaissance se déroulerait à court terme.

En Allemagne, la loi dite du Signaturgesetz (Art. 3 luKDG) se limite à la reconnaissance de l'utilisation de la signature numérique par les personnes physiques par le biais d'un chiffrement à clé publique. Le législateur met dès lors à disposition une "norme" constitutive d'une présomption légale, qui n'est toutefois pas obligatoire. Dès lors, nous avons affaire dans ce cadre à un système facultatif, en ce sens que l'Allemagne propose une norme en matière de signature numérique. Si cette norme est utilisée, il y a de fortes raisons de croire que le juge acceptera cette signature comme étant une signature probante.

Des discussions sont à l'heure actuelle menées en vue d'édicter une directive européenne qui concilierait les points de vue précités.

En Belgique, le Conseil des Ministres a décidé le 30 mai 1997 de réglementer la signature numérique et d'adapter le Code Civil. En 1998, deux projets de loi en ce sens ont été rédigés.

De l'exposé des motifs du projet de loi visant à adapter le Code Civil, il semble que le but principal poursuivi est d'adapter les règles de preuve du Code Civil aux besoins de la société de l'information et, plus précisément, à l'échange et à l'archivage de données par voie électronique, sans cependant réformer fondamentalement les principes essentiels de notre droit de la preuve.

Si l'écrit est une composante essentielle de l'acte sous seing privé, c'est toutefois la signature qui lui procure pleine valeur juridique.

A l'art. 1322 du Code Civil est ajouté un nouvel alinéa où il est disposé qu'outre la signature manuscrite apposée directement sur l'écrit, *“l'ensemble de données issues de la transformation de l'écrit et dont ressort avec certitude l'identité de l'auteur et son adhésion au contenu de l'écrit”* peut également constituer une signature.

Cette disposition doit faire en sorte qu'en cas de contestation sur l'établissement de la preuve d'un acte, le juge puisse également considérer une signature électronique comme une signature au sens du Code Civil.

Afin d'éviter l'obligation d'introduire dans le Code Civil des concepts totalement nouveaux comme “document” ou “information”, ce qui pourrait porter atteinte à la cohérence du code, le projet maintient la notion “d'écrit”. Cette notion n'a nulle part été définie expressément dans le Code Civil, mais la jurisprudence et la doctrine s'accordent de plus en plus pour considérer qu'il convient de l'interpréter de façon large et qu'il ne faut pas considérer comme “écrit” le seul texte manuscrit ou imprimé sur un support papier.

Dans la disposition proposée, il est ensuite exigé que “l'ensemble de données” trouve son origine dans la transformation - généralement mathématique - de l'écrit, de sorte que s'établisse un lien indissociable entre l'écrit et la signature.

Enfin, deux exigences fonctionnelles supplémentaires sont ajoutées, à savoir que “l'ensemble de données” fasse apparaître :

- l'identité de l'auteur de l'écrit, et
- son adhésion au contenu de l'écrit

Monsieur Patrick Van Eecke : “Protection des communications privées” (K.U. Leuven - Centre Interdisciplinaire Droit et Informatique)

L'art. 79 de la loi du 19 février 1997 modifiant la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, insère dans cette loi un art. 109ter F qui stipule que l'emploi de la cryptographie est libre.

Le cryptage est une technique qui consiste à rendre les informations incompréhensibles pour des tiers. Le cryptage ou “codage” n'est pas lié au média de télécommunication et peut être utilisé tant pour le “chiffage” des conversations par le biais d'un téléphone fixe ou sans fil que pour rendre incompréhensibles les échanges par fax ou internet. Cette technique visant à garder la confidentialité des messages a déjà été utilisée de tout temps, au sein des milieux tant militaires que civils.

En l'absence de protection, les messages qui sont transmis par le biais de réseaux publics peuvent en effet être interceptés et même manipulés sans trop de problèmes. Le risque de voir des autorités hostiles ou des entreprises concurrentes se procurer un accès à ces informations n'est pas inconcevable et incite dès lors à recourir à une protection importante telle le cryptage.

Il est ainsi possible, sur base de la même technique, de garantir également l'intégrité du message. Il est important que le message lui-même ne doive pas être codé pour pouvoir en garantir l'intégrité. La signature digitale est une forme dérivée de cryptage qui, à l'avenir, gagnera certainement en importance. La signature digitale est le plus souvent une adjonction au message, fondée sur l'information et sur une clé secrète. Le destinataire du message peut vérifier la signature en faisant usage d'une clé publique.

Il est incontestable que la protection des informations constitue un élément indispensable dans le cadre du développement de la société d'information. Le recours au cryptage présente toutefois également un revers. Le milieu criminel peut en effet également recourir à cette méthode pour rendre ses données illisibles. Bien que le codage d'informations existe depuis toujours l'importance des progrès de la technologie du cryptage entraîne l'usage répandu de mécanismes de codage de plus en plus puissants. Il devient, toutefois, impossible pour les autorités de libérer les moyens nécessaires dans ce domaine.

Du point de vue judiciaire, la nécessité d'entreprendre une action régulatrice s'impose dès lors. Une prise de décision en la matière nécessite de prendre en considération les différents intérêts en présence, à savoir le droit à la confidentialité de l'information et la nécessité de protéger la société contre les comportements criminels.

L'interdiction totale du cryptage, assortie ou non d'exceptions, a déjà été proposée par quelques pays comme solution pour réaliser un contrôle efficace par l'autorité.

Une interdiction générale du cryptage est toutefois difficilement défendable pour diverses raisons. A côté du droit à la vie privée, tel qu'il résulte de l'article 8 de la Convention Européenne des droits de l'homme, on doit également prendre en considération les aspects économiques et financiers. L'utilisation du cryptage est en effet considérée comme un élément indispensable pour la protection des informations.

Une interdiction du cryptage aurait en outre peu d'effet. Il est par ailleurs souvent impossible de vérifier si un message est crypté ou non.

D'autres pays autoriseraient le chiffrement à la condition que la clé de chiffrement fasse l'objet d'un dépôt.

Ce contrôle peut avoir lieu soit par une déclaration a priori des clés aux autorités, soit par une déclaration à un tiers de confiance.

Le dépôt des clés ne paraît, toutefois, pas être une bonne manière de résoudre le problème du cryptage. C'est une procédure très compliquée et très onéreuse qui oblige l'organe de gestion (les autorités ou les tiers de confiance) à disposer d'une infrastructure importante. L'organe de gestion constitue, en effet, une cible de choix pour les éléments malhonnêtes et doit dès lors répondre à des conditions de protection extrêmement élevées.

Dans le cas où chaque utilisateur de mécanismes de cryptage serait obligé de faire connaître sa clé aux autorités, le citoyen moyen se soumettrait à cette obligation mais le crime organisé, pourtant visé par la mesure, passerait à travers les mailles du filet.

Même en cas de régulation du cryptage, il sera d'ailleurs très difficile d'intercepter des messages électroniques.

D'un point de vue économique, on ne peut qu'applaudir à la libéralisation de l'utilisation du chiffrement telle qu'elle est à l'heure actuelle prévue par la loi en Belgique. La Belgique est en effet le seul état européen à adopter pareille position. La liberté d'utilisation des techniques de chiffrement est dès lors admise de manière explicite.

Du point de vue judiciaire également, l'usage répandu du cryptage augmentera l'efficacité de la prévention du crime. Les informations sont en effet protégées contre la prise de connaissance non autorisée et la manipulation, ce qui diminue le risque d'espionnage industriel, d'escroquerie ou de sabotage.

Il faut toutefois admettre que la loi sur les écoutes est ainsi déforcée.

Les dispositions du projet de loi relatif à la criminalité informatique prévoient cependant que le juge d'instruction a le droit de requérir l'aide de toute personne disposant de connaissances pour l'aider à déchiffrer, à l'exclusion des suspects et de la famille proche.

On doit aussi comprendre que l'évolution des nouvelles méthodes de télécommunication offre également des possibilités aux autorités chargées de l'enquête. Il est ainsi devenu plus facile, en consultant des banques de données électroniques, de retrouver des personnes ou d'établir des liens entre les infractions; de même, des communications téléphoniques peuvent être plus rapidement localisées, etc... .

De manière globale, on peut donc dire que les désavantages sont compensés par la protection préventive d'informations importantes et par les nouvelles techniques d'enquête.

CHAPITRE 2 : RAPPORT DE LA PARTICIPATION D'UN MEMBRE DU COMITÉ R AU SÉMINAIRE “L'ANALYSTE D'IMAGES, AU COEUR DU SYSTÈME D'OBSERVATION SPATIALE” ORGANISÉ À MADRID LES 15 ET 16 OCTOBRE 1998.

Dans la foulée de l'enquête qu'il a menée sur la participation des services de renseignement belges à des programmes satellitaires de renseignement ⁽¹⁾, le Comité R a souhaité maintenir son attention pour ce sujet.

Un de ses membres a donc assisté au séminaire “*l'analyste d'images, au coeur du système d'observation spatiale*” organisé à Madrid les 15 et 16 octobre 1998. Le sujet de ce séminaire rencontrait tout-à-fait les préoccupations du Comité R puisque celui-ci avait notamment recommandé de mettre en place un centre d'analyse d'images satellitaires au SGR et de former du personnel qualifié à cette fin, ce qui signifie la mise en oeuvre de moyens matériels et humains adéquats.

Ce séminaire de Madrid a été organisé pour célébrer le cinquième anniversaire du centre satellitaire de l'Union de l'Europe occidentale situé à Torrejón (Madrid - Espagne). Cette rencontre internationale, placée sous la présidence de Monsieur José Cutileiro, Secrétaire général de l'UEO, et avec la participation de Monsieur Eduardo Serra, Ministre de la Défense du Royaume d'Espagne, a réuni quelques uns des plus grands spécialistes européens, américains et russes de l'exploitation d'images spatiales.

L'apport humain des analystes d'images était le thème central de ce colloque.

Les méthodes d'analyse d'images doivent constamment s'adapter à l'évolution rapide de la technologie des capteurs (ou senseurs). De nouveaux instruments sont à présent capables d'observer la terre de différentes manières et de produire des “images” qui ne correspondent pas nécessairement au mode de perception de l'oeil humain : par exemples, par rayons X, par rayons infra-rouge, par ondes radio métriques, par rayonnement radar, etc De plus, la sensibilité (ou la résolution) de ces capteurs ne cesse de s'affiner. Tous ces moyens d'observation se complètent et permettent de couvrir de larges zones à toute heure (de jour, comme de nuit), par tous les temps, aussi bien pour détecter des objectifs spécifiques que pour observer l'évolution d'une situation.

Les données obtenues par les différents types de capteurs spatiaux ne sont pas seulement complémentaires les unes des autres, elles se conjuguent également à toutes les autres informations obtenues par les méthodes classiques de recueil du renseignement (sources humaines, techniques, reconnaissance aérienne, informations collatérales obtenues à partir de sources ouvertes, etc...).

(1) Comité R - rapport d'activités 1998 - p.130

Rassembler et traiter correctement l'immense quantité des données fournies par ces différents types de senseurs et autres sources d'informations est donc devenu un problème crucial pour l'établissement de rapports d'analyse et la prise de décision. Même un équipe performante d'analystes chevronnés risque bientôt de ne plus être en mesure d'effectuer une analyse complète et détaillée de toutes les données recueillies par ces nombreuses espèces de capteurs.

D'autre part, les analystes du 21ème siècle vont être confrontés à des demandes d'informations de plus en plus précises et pressantes de la part des preneurs de décisions. Ces demandes concerneront de vastes domaines, allant de la sécurité à l'environnement, partout dans le monde. Les analystes devront être capables de traiter, d'analyser et d'interpréter presque en temps réel un immense flot de données dont ils devront retirer et présenter le renseignement utile à la prise de décision.

Parallèlement à cette évolution complexe des capteurs, des logiciels informatiques de plus en plus nombreux et sophistiqués ont été mis au point pour aider les analystes d'images à traiter les énormes flots de données numériques. L'US Air Force (USAF) semble être très avancée dans ce domaine.

De quelle manière l'homme peut-il encore travailler efficacement dans un tel contexte ? La technologie va-t-elle remplacer l'homme ? Quelles sont les limites des logiciels d'analyse ? Quelles sont les qualités requises de la part d'un bon analyste d'images ? Quels sont les processus cognitifs que celui-ci met en oeuvre pour effectuer son travail ? De quelles manière faut-il sélectionner et former les analystes d'images ? Comment améliorer leur efficacité et leur productivité ? Comment conserver et valoriser le savoir-faire des analystes qui quittent la profession ? Comment un analyste peut-il se tenir à jour dans sa formation et suivre l'évolution des technologies ? Telles furent quelques unes des multiples questions abordées au cours du colloque de Madrid.

En règle générale, tous les orateurs estiment que malgré les développements technologiques en cours, le facteur humain, c'est-à-dire le savoir-faire et l'expérience des analystes d'images, reste primordial. Le travail en équipes pluridisciplinaires s'impose de plus en plus. Enfin, la technique doit rester au service de l'analyste et non l'inverse.

Les modes de formation des analystes ont été abondamment discutés. On retiendra qu'il existe des programmes de formation internationaux soit dans le cadre de l'OTAN, soit dans le cadre d'accords bilatéraux. Il existe également des écoles privées et des modules de formation circulent sur INTERNET.

D'autres sujets plus techniques tels que la haute résolution des capteurs, la troisième dimension, les compréhension et l'usage des images radars (micro-ondes), l'usage de l'intelligence artificielle dans l'analyse d'images, etc ... ont été abordés. Parmi les intervenants, le belge Marc Acheroy, professeur à l'école royale militaire, a traité de l'analyse des images spatiales par fusion des données multispectrales.

En conclusion, le Comité R répète qu'il serait essentiel que le gouvernement belge crée sa propre cellule d'analyse d'images satellitaires. Une telle cellule est indispensable comme outil d'aide à la prise de décision dans des matières internationales telles que l'envoi de forces armées à l'étranger, la participation à des opérations de maintien de la paix, l'aide humanitaire, la prévention et la gestion de catastrophes écologiques.

CHAPITRE 3 : COMPTE-RENDU DU COLLOQUE

“SECRET D’ETAT OU TRANSPARENCE ?”

20 JANVIER 1999

Comme l’écrit l’amiral Lacoste, ancien directeur de la Direction générale de la sécurité extérieure (DGSE - France), “A une époque où les principes démocratiques et les droits de l’homme sont de plus en plus reconnus comme des valeurs universelles, les citoyens de tous les pays tendent à exiger de leurs gouvernements la transparence dans la conduite des affaires publiques. Beaucoup sont réticents à admettre que les hommes politiques et les administrations puissent arguer du “Secret d’Etat” pour dissimuler certaines informations à leurs concitoyens. Au delà des aspects sensationnels ou des polémiques portant sur des cas particuliers, il s’agit bien là d’un sujet capital, car il est éminemment politique, au sens noble du mot. C’est un débat de société qui ne devrait laisser personne indifférent” ⁽¹⁾.

C’est sur base de cette réflexion que le Comité R décida de stimuler ce débat de société en organisant le 20 janvier 1999, un colloque intitulé “*Secret d’Etat ou transparence ?*”. Cette manifestation a été mise sur pied en collaboration avec le Centre d’Etudes de Défense de l’Institut Royal Supérieur de Défense (IRSD). Elle fut organisée dans la foulée de la publication de l’étude du Comité R sur *les devoirs de secret auxquels sont tenus les membres des services de renseignements*”.

L’objectif était aussi de sensibiliser les mondes politique, judiciaire, académique, les militaires et les agents des services publics sur la nécessité de légiférer en cette matière dans un environnement international en mutation.

Le Comité R a donc réuni un panel d’orateurs choisis parmi des personnalités belges et étrangères connues pour leurs compétences dans cette matière.

Les orateurs belges de ce colloque ont été le ministre de la Défense nationale Jean-Pol Poncelet, le député Jan Van Erps, l’avocat Anne Krywin, le journaliste Walter De Bock, le professeur Yves Pouillet et le conseiller d’Etat Robert Andersen.

Les invités de marque étrangers ont été l’Amiral français Pierre Lacoste, l’éminent juriste britannique David Bickford, le professeur néerlandais Ton Beers et Monsieur Rémi Hyppia, chef de projet au Comité canadien de surveillance des activités de renseignement de sécurité.

(1) “*Justification et légitimité du secret d’Etat*” - cahier n° 12 de la fondation pour les études de défense (1998).

L'intervention de chacun se résume dans les quelques lignes qui suivent.

Monsieur Jean-Pol Poncelet, vice-premier ministre et ministre de la Défense nationale

C'est à Monsieur Jean-Pol Poncelet, vice-premier ministre et ministre de la Défense nationale, que revint l'honneur de prononcer l'allocution d'ouverture du colloque. Celui-ci s'est déclaré régulièrement confronté à la tension qui existe entre la nécessité de préserver les secrets d'Etat et celle d'informer le Parlement, l'opinion publique et la presse. La tension entre le secret d'Etat et la transparence soulève les questions suivantes :

- S Quelles menaces la société de l'information fait-elle peser sur la protection des secrets d'Etat ?
- S Comment résoudre le paradoxe actuel d'une demande croissante de transparence dans la gestion des affaires publiques allant de pair avec une revendication de plus en plus forte de protection du secret de la vie privée ?
- S Jusqu'où le secret d'Etat est-il légitime, et comment organiser le contrôle de cette légitimité ? Comment, enfin, atteindre un juste équilibre entre secret d'Etat et transparence ?

Amiral Lacoste (France) - "Justifications et légitimité du secret d'Etat".

Pierre Lacoste est entré dans la marine française en 1943; c'est dans ce corps d'armée qu'il a fait carrière jusqu'au grade d'amiral affecté au commandement de l'escadre de la Méditerranée.

En 1982, l'amiral Lacoste a pris la tête de la DGSE, la Direction générale de la sécurité extérieure, qui est le service français de renseignement et d'action extérieur.

En 1985, le sabotage du Rainbow Warrior, le bateau du mouvement écologiste Greenpeace, a mis fin à sa carrière à la DGSE.

Depuis 1986, Pierre Lacoste se consacre aux activités d'études et de réflexion sur les grands problèmes de Défense, notamment à l'Université de Marne-la-Vallée où il dirige une formation intitulée "information-sécurité".

Avant de rappeler les principales justifications qui légitiment l'existence et les pratiques du secret d'Etat (secret militaire, conduite de la politique étrangère, sûreté de l'Etat et sécurité intérieure), l'Amiral Lacoste a souligné le fait que le concept du "secret" en général, soulève un grand nombre de questions dont beaucoup sont particulièrement complexes. Il a traité des évolutions actuelles du secret d'Etat en France, et pour conclure, a esquissé quelques perspectives du monde contemporain.

David Bickford (Royaume Uni) - “Balanced secrecy in the new information age”.

David Bickford est un éminent juriste britannique et consultant en matière de lutte contre le crime organisé, la délinquance économique et le blanchiment d'argent.

Auparavant, M. Bickford a occupé de hautes fonctions au Ministères des Affaires étrangères de Grande Bretagne; il a été membre du Collège des directeurs et conseiller juridique des services secrets du Royaume Uni (MI5 et MI6).

En cette qualité, il a été l'un des promoteurs des lois de 1989 et de 1994 connues sous les noms de “*Security Service Act*” et de “*Secret Intelligence Service Act*”.

Selon David Bickford, le secret d'Etat doit à présent faire face aux nouveaux défis de l'ère de l'Information et du développement du commerce mondial par l'internet. Ces défis vont de pair avec ceux de l'internationalisation du crime organisé et de nouvelles menaces.

Dans ce nouveau monde virtuel, il faudra déterminer avec soin ce qui, dans chaque domaine, doit rester secret. Une conception trop large du secret ne résistera pas aux nouveaux besoins de la société.

Si l'on veut combattre efficacement les nouvelles menaces, les services de renseignement devront travailler en très étroite collaboration avec les services de police.

Pour M. Bickford, les problèmes qui se posent dans cette collaboration sont les suivants :

- S La tâche des services de renseignement consistera à collecter le plus d'informations possible sur, notamment, les organisations criminelles et ceci, en faisant usage de toutes les méthodes dont ces services dépendent (informateurs, écoutes téléphoniques, ...).
L'objectif est de transformer ces renseignements en preuves utiles. Comment donc utiliser une information classifiée comme moyen de preuve devant un tribunal ? Et M. Bickford d'illustrer ces questions par quelques exemples tirés des procédures en vigueur au Royaume-Uni et en France.

- S Le besoin d'informations exprimé par la société aura comme conséquence qu'une instance d'arbitrage indépendante du gouvernement devra être chargée de distinguer ce qui est un secret vital de ce qui ne l'est pas.

Les problèmes qui peuvent se poser au niveau des très nombreuses informations échangées entre agences internationales sont également évoqués par M. Bickford.

L'orateur estime notamment que les Etats devraient harmoniser leurs conceptions du secret et accepter de le réduire au minimum vital, sous peine de le voir emporté par les nouveaux besoins de la société.

M. Ton Beers (Pays Bas) - “Un modèle d’analyse juridique”.

Ton Beers est professeur de droit public et de droit de l’information à la faculté de droit de l’Université Catholique du Brabant, à Tilburg aux Pays Bas.

En 1984 et 1997, il a analysé et commenté la jurisprudence des tribunaux en matière de publicité de l’administration, ceci pour compte du ministère de l’Intérieur. Il a été consulté dans cette matière par la Commission européenne et par des gouvernements étrangers.

M. Beers constate qu’au cours des deux dernières décénies, la publicité de l’administration est devenue la règle dans la plupart des démocraties occidentales, le secret, l’exception.

Le secret n’est légitimé que s’il repose sur une règle de droit qui soit à la fois publique et suffisamment prévisible. Cette règle doit aussi être nécessaire dans une société démocratique pour protéger certains intérêts publics et privés.

L’intérêt de la transparence et l’intérêt du secret ne sont pas absolus : ils doivent être soupesés de manière équilibrée. L’intérêt de la transparence comporte en fait un certain nombre d’intérêts différents.

M. Rémi Hyppia (Canada) - “Peut-on protéger les secrets d’Etat tout en faisant preuve de transparence ?”

M. Hyppia est docteur en science politique de l’université du Québec à Montréal.

Il exerce la fonction de chef de projet auprès du Comité de surveillance des activités de renseignement de sécurité depuis janvier 1998. Ce comité est en quelque sorte l’équivalent du Comité R au Canada. M. Hyppia a rendu compte de son expérience au sein de cet organe de surveillance qui a la tâche délicate de concilier la confidentialité nécessaire à l’efficacité du service de renseignements canadien avec son devoir de transparence envers le Parlement et le peuple canadiens. Cette double exigence donne lieu chaque année, lors de la préparation du rapport annuel, “à des prouesses d’équilibre entre la transparence et la protection du secret d’Etat”.

M. le député Jan Van Erps - “Présentation du projet de loi relatif à la classification et aux habilitations de sécurité”.

Le député Jan Van Erps a siégé dans la commission de la Défense nationale; à ce titre il a été rapporteur du projet de loi relatif à la classification et aux habilitations de sécurité.

L'orateur a expliqué comment les amendements introduits par la commission lors de la discussion du projet de loi, ont abouti à concilier la loi du 11 décembre 1998 ⁽²⁾ avec les nouveaux droits à la publicité de l'administration et à la vie privée.

Madame Anne Krywin - "Le secret d'Etat et les droits de l'homme".

Anne Krywin est avocate au barreau de Bruxelles, spécialiste en droit pénal. Elle est aussi présidente de la commission "Justice" de la Ligue des droits de l'homme.

A ce titre, elle souligna l'importance qu'avait pris le principe du droit de la défense dans les limites au pouvoir des organes de l'état chargés de la prévention et de la répression. Il faut que le prévenu ait eu le loisir de contredire, devant les juridictions de jugement, les éléments apportés contre lui par le ministère public. Le respect de ce principe pose la question de l'information apportée aux tribunaux par les services de renseignement. *"Comment contredire ce qui par essence doit être tenu secret, une infiltration, une provocation, une méthode déloyale ?"*

Pour l'orateur, le vide juridique en ce qui concerne l'accès éventuel à des dossiers relevant du secret d'Etat fait apparaître la nécessité d'une intervention législative. En attendant, Me Krywin espère que les autorités de contrôle (magistrature assise, Comité R ou parlement) resteront vigilantes à ce que les services de renseignement soient soumis à un contrôle effectif de leurs activités.

Walter De Bock, journaliste

Monsieur De Bock est journaliste professionnel depuis 1972. Il a notamment travaillé comme rédacteur auprès d'un hebdomadaire politique et économique, ainsi que comme collaborateur à des programmes d'information de la BRT.

Depuis 1979, il se penche sur des dossiers politiques, judiciaires et financiers dans les colonnes d'un quotidien flamand. Il est auteur et co-auteur de différents ouvrages.

L'orateur évoque ses premières expériences journalistiques qui, au début des années "80", l'ont mis en rapport avec l'information sur les services de renseignements belges. Partant des difficultés auxquelles la Sûreté de l'Etat fut confrontée au cours de ces années, M. De Bock estime que les services de renseignements défensifs, surtout comme ceux qui existent dans des petits pays comme la Belgique, ont tout à gagner à fonctionner de manière claire et respectueuse des règles d'un état de droit démocratique.

⁽²⁾ M.B. 07/05/1999

Selon, M. De Bock, si les problèmes d'alors de la Sûreté de l'Etat sont devenus aussi inextricables, c'est parce que ce service n'avait, dans ces années de crise, pratiquement pas de statut légal et qu'il ne disposait pas encore d'un cadre administratif et déontologique clair, ni d'ailleurs d'aucune forme de contrôle extérieur.

C'est donc cette crise autour et au sein de la Sûreté de l'Etat qui a fait apparaître l'urgence pour le législateur de se mettre au travail afin de combler un vide juridique de 150 ans en la matière. C'est ainsi que l'état de droit progresse à petits pas.

C'est grâce à la transparence et à la publicité de l'administration que l'opinion publique peut s'assurer que les services de renseignements restent sous le contrôle d'un état de droit démocratique.

M. Yves Poulet - "Secret d'Etat et vie privée : ou comment concilier l'inconciliable ?"

Monsieur Yves Poulet est docteur en droit, professeur aux Facultés Universitaires Notre-Dame de la Paix à Namur. Il y enseigne notamment les libertés individuelles. Il est aussi directeur du Centre de Recherches Informatique et Droit.

Ses thèmes de recherche favoris concernent le droit des nouvelles technologies de l'information et de la communication. Ses compétences particulières dans ces domaines lui valent de siéger au sein de la Commission de protection de la vie privée.

M. Poulet entend démontrer que dans un grand nombre d'hypothèses, secret d'Etat et protection de la vie privée peuvent s'épauler mutuellement. *"La personne fichée a tout intérêt à ce que les données la concernant soient aussi bien protégées que possible contre la diffusion à des tiers non autorisés"*.

La particularité des missions des services de renseignement et de sécurité réclame aussi que les multiples limites aux modes de collecte et au traitement des données affirmées par les législations protégeant la vie privée soient parfois oubliées au profit de l'efficacité légitime des services en cause. Mais pour qu'elles soient et restent légitimes, la Cour européenne des droits de l'homme exige que ces exceptions soient "prévues par la loi" et restent proportionnées aux nécessités de l'action qui les fondent.

Enfin, l'orateur estime que l'intervention d'une autorité indépendante en la matière n'est pas suffisamment développée par la législation belge puisque la commission de la protection de la vie privée n'a pas les moyens d'un contrôle effectif sur l'action des services de renseignement.

M. Robert Andersen - “La mise en balance des intérêts en cause dans l’appréciation des motifs d’exception à la publicité de l’administration”

Monsieur Robert Andersen est président de chambre au Conseil d’Etat. Mais c’est surtout en sa qualité de président de la Commission fédérale d’accès aux documents administratifs (la CADA) que l’intéressé a été convié à participer au colloque.

Le droit d’accès aux documents administratifs est à présent un droit fondamental du citoyen. Ce droit n’est toutefois pas garanti inconditionnellement. Des exceptions peuvent y être apportées par voie législative. On se trouve alors en présence d’un conflit entre, d’une part, le droit fondamental d’accès aux documents administratifs et, d’autre part, d’autres valeurs jugées essentielles dans un Etat démocratique.

Tantôt le législateur résout lui-même le conflit lorsque le principe de la publicité doit céder le pas à des valeurs considérées comme étant supérieures. Tantôt le législateur laisse à l’administration elle-même le soin de procéder à la mise en balance des intérêts en présence et de décider, dans chaque cas d’espèce, de la solution à donner au conflit.

Certains motifs d’exceptions à la transparence sont absolus, d’autres sont relatifs. Un contrôle est alors nécessaire; celui-ci doit pouvoir s’exercer par une instance indépendante de celle qui a pris la décision motivée. Et M. Andersen de commenter un certain nombre de décisions prises en la matière par la CADA.

Bien que des résistances se fassent encore sentir çà et là, la tendance vers une plus grande publicité de l’administration semble irrésistible. L’orateur ne peut que s’en réjouir.

CHAPITRE 4 : RAPPORT SUCCINCT RELATIF À LA PARTICIPATION DU COMITÉ R À LA CONFÉRENCE DES ORGANISMES DE SURVEILLANCE DES ACTIVITÉS DE RENSEIGNEMENT, S'ÉTANT TENUE À OTTAWA LES 28 ET 29 JUIN 1999 SUR LE THÈME : "EXAMEN ET SURVEILLANCE DANS LE NOUVEAU MILLÉNAIRE : LES DÉFIS D'UN MONDE MULTIPOLAIRE."

Le Comité R a été invité à participer à la seconde édition de cette réunion bisannuelle, qui s'est tenue pour la première fois en Australie en 1997.

Les exposés, suivis de débats, se sont déroulés durant deux journées dans la capitale Canadienne et ont porté sur quatre thèmes principaux choisis par les organisateurs, à savoir :

- S problèmes et conditions spécifiques rencontrés dans le champs d'activité;
- S transparence et sécurité nationale, rapports avec le monde politique;
- S transparence et sécurité nationale, rapports avec les médias;
- S ressources indispensables au contrôle : compétences et personnel.

Participaient à ce forum international, outre les délégations canadienne et belge, des représentants d'organismes de contrôle (interne ou externe) du Royaume-Uni, d'Australie, de Nouvelle-Zélande, d'Afrique du Sud et des U.S.A.

Il est à noter que certains pays ont organisé un double système de contrôle, cumulant de la sorte l'organisme de surveillance interne (par ex : la fonction d'inspecteur général au sein du service) et l'organisme de surveillance externe (par ex : une commission parlementaire ou un comité non parlementaire, instaurés par la loi et désignés, selon le cas d'espèce, par le Pouvoir Exécutif ou par le Parlement).

Il ressort, en résumé, de la confrontation des expériences de chacun que la problématique est identique, qu'il s'agisse de contrôler de petits ou de grands services. Tous les services considérés sont décrits comme attachés à leur culture du secret et naturellement peu enclins à intégrer le contrôle.

De même la communication aux assemblées parlementaires de chaque pays représenté (y compris ceux dont la surveillance est exercée par une commission composée d'élus) de la totalité des informations recueillies au cours des enquêtes de contrôle pose problème au niveau des garanties de confidentialité.

Quant au rôle des médias, il est ressorti des échanges de vues que tous les participants souhaitent qu'une certaine transparence s'installe, pour autant qu'elle ne porte pas atteinte à l'efficacité des services. A cette condition les services de renseignement et de sécurité devraient d'ailleurs bénéficier de la part du grand public d'une meilleure compréhension de la nécessité de leurs missions.

En résumé, tant à l'égard du monde politique que des médias, un - délicat - équilibre doit s'instaurer, qui préserve le contrôle démocratique sans pour autant nuire à la bonne exécution des missions.

Globalement enfin, les organismes de surveillance qualifient généralement de satisfaisants les moyens qui leur sont donnés en rapport avec le contenu de leur activité. Il faut néanmoins noter que le degré de satisfaction dépend des spécificités propres à chaque pays. C'est ainsi, par exemple, qu'un pays disposant déjà d'un contrôle interne efficace pourra affecter moins de moyens à son contrôle externe, ce en raison des interactions développées.

Le "Comité R" conclut donc, à l'issue de la confrontation de son expérience propre à celle d'autres organismes de contrôle à l'étranger, à l'existence d'une constante : quelle que soit la structure mise en place, l'exercice d'un contrôle sur les services de renseignement constitue partout une source de tensions donnant lieu à de délicats exercices d'équilibre entre la spécificité de leurs missions et la transparence due au Parlement et au public.

Tous les participants ont manifesté le souhait qu'une nouvelle conférence d'évaluation ait lieu dans deux ans et les représentants du Royaume-Uni aimeraient l'organiser sur leur sol en 2001.

CHAPITRE 5 : RAPPORT SUCCINCT RELATIF À LA PARTICIPATION DU COMITÉ "R" AUX JOURNÉES D'ÉCHANGE DE VUES ORGANISÉES LES 6 ET 7 SEPTEMBRE 1999 À BUCAREST À L'INITIATIVE DES COMMISSIONS PARLEMENTAIRES ROUMAINES DE SUIVI DES SERVICES DE RENSEIGNEMENTS

Le Parlement Roumain a invité le Comité "R" à confronter son expérience du contrôle des services de renseignement belges avec celle de l'organe de suivi Roumain, constitué d'une "Commission Permanente Commune" créée en 1993 et composée de sept députés et de deux sénateurs, compétente pour le "SRI" ("Serviciul Roman de Informatii" : service **intérieur**, c'est-à-dire dont les activités ⁽¹⁾ s'exercent exclusivement sur le territoire national), et d'une *Commission ad hoc* créée en 1997 et composée de deux sénateurs et trois députés (issus des commissions de la Défense nationale, l'Ordre Public et la Sécurité Nationale) compétente pour le "SIE" ("Serviciul de Informatii Externe", service **extérieur**, c'est à dire dont les activités sont centrées sur le renseignement à l'étranger concernant la sécurité nationale et la sauvegarde des intérêts roumains.)

Le Directeur du SRI est un ancien parlementaire, démissionnaire pour la cause, nommé à ce poste par décision du Président de la République nécessitant toutefois validation par les deux chambres législatives. Le Directeur du SIE est, quant à lui, désigné par le Conseil Suprême de Défense du Pays sur présentation du Président de la République. Tous deux ont rang de ministre et chaque service constitue une Autorité administrative autonome.

Après avoir porté cette invitation à la connaissance des Présidents du Sénat et de la Chambre des Représentants, par lettres du 27 mai 1999, le Comité "R" a accepté la proposition avec d'autant plus d'intérêt que le contrôle parlementaire mis en place en Roumanie a été, tout comme la Constitution Roumaine, largement inspiré du modèle belge.

Les séances d'exposés se sont déroulées dans l'enceinte du Parlement, au siège de la "Commission Permanente Commune", et ont été présidées par Monsieur Nicolae Ionescu-Galbeni, M.P., en sa qualité de Président de ladite commission. A l'issue de ceux-ci des échanges de vue approfondis se sont noués entre les participants.

(1) Collecte et traitement des renseignements indispensables à la connaissance, à la prévention et à la lutte contre les actions portant atteinte à la sécurité de la nation roumaine; défense des secrets et prévention de la fuite de renseignements non autorisés à la publication; interventions anti-terroristes et protection des "V.I.P."; ... et caetera

Parmi les très nombreuses informations reçues, le Comité "R", à la lueur de sa propre loi organique, a :

1. relevé - notamment - la composition proportionnelle pluraliste de l'organe de contrôle roumain ainsi que des modes et conditions de désignation de ses membres;
2. analysé le contenu de son rôle de vérificateur de la constitutionnalité et de la légalité des activités des services;
3. pris acte du suivi budgétaire permanent mis en place, de sa compétence en matière de plaintes émanant de citoyens s'estimant lésés, du contrôle via les destinataires d'informations et de l'obligation faite à cette Commission de présenter annuellement au Parlement un rapport d'activité.

De leur côté les sénateurs et députés roumains, membres des commissions "intérieure" et "extérieure", ont marqué leur vif intérêt pour le rôle que joue le Comité "R" comme organe de contrôle des services de renseignement, pour compte du parlement, devant lequel il fait rapport régulier par le truchement des commissions de suivi parlementaire. Ils ont été attentifs à la description de l'obligation de secret faite aux membres du Comité "R" et aux sanctions pénales s'attachant à la violation éventuelle de celle-ci. Ils ont évoqué la culture du secret pratiquée par les services et la difficulté rencontrée par certains membres des commissions Roumaines, absorbés par d'autres tâches et non spécialisés, d'exercer effectivement le devoir de contrôle sans pour autant nuire à l'efficacité des services.

Dans cet ordre d'idées, l'existence aux côtés du Comité "R", d'un Service d'enquêtes, par ailleurs doté de compétences judiciaires lorsqu'il agit pour compte du procureur général ou d'un juge d'instruction, a paru séduisante aux membres des Commissions .

Le rôle des médias a lui aussi été abordé dans une préoccupation constante d'équilibre entre plus grande transparence et garantie d'opérationnalité des services.

En bref, le Comité "R" a une fois de plus constaté que la problématique s'avère identique quelle que soit la taille, la mission, ou l'origine nationale des services considérés, tandis que les deux commissions roumaines se sont dites intéressés à poursuivre les échanges avec le Comité "R" et la commission de suivi parlementaire belge.

TITRE IV : HISTORIQUE DU COMITE R

COMPOSITION ET FONCTIONNEMENT DU COMITE PERMANENT R

COMPOSITION DU COMITÉ PERMANENT R

La loi du 18 juillet 1991 prévoyait que le Comité permanent R était composé de cinq membres permanents, dont un président et un vice-président, et de cinq membres suppléants, tous nommés alternativement par la Chambre des représentants et par le Sénat qui pouvaient aussi les révoquer.

Au cours de la session parlementaire 1998-1999, le Comité permanent R a été composé de quatre personnes, le mandat laissé vacant par la démission de Monsieur Decoux en octobre 1995 n'ayant jamais été pourvu. En outre, la composition du Comité permanent R a connu quelques modifications.

Le 4 novembre 1998, Monsieur Jean-Louis Prignon, juge d'instruction et membre suppléant du Comité permanent R, a prêté serment en qualité de membre effectif pour achever le mandat de Monsieur Guy Collignon, démissionnaire le 16 octobre 1998.

Le 21 décembre 1998, la présidente du Comité permanent R, Madame Véronique Paulus de Châtelet, a présenté sa démission de ses fonctions de présidente du Comité permanent R pour être nommée en qualité de gouverneur de l'arrondissement administratif de Bruxelles-capitale.

Madame Danielle Cailloux, membre effectif du Comité permanent R, a alors exercé provisoirement les attributions de présidente.

Le 2 février 1999, Monsieur Jean-Claude Delepière, substitut du Procureur du Roi au parquet de Bruxelles, membre et président suppléant de la cellule de traitement des informations financières et président suppléant du Comité permanent R, a prêté serment en qualité de président effectif pour achever le mandat laissé vacant par Madame Paulus de Châtelet.

Depuis lors, le Moniteur belge du 3 avril 1999 a publié la loi du 1^{er} avril 1999 modifiant la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements. Cette loi réduit la composition du Comité permanent R à un seul membre effectif permanent, qui en est le président, et à deux membres effectifs non permanents. Un suppléant est nommé pour chacun d'eux. Désormais, seul le président du Comité permanent R exercera son mandat à temps plein.

L'article 41, alinéa 2 de la loi du 1^{er} avril 1999 dispose en outre que "*la nomination des membres du Comité permanent R qui sont en fonction à la date d'entrée en vigueur de la présente loi prend fin à la nomination des nouveaux membres*".

A la date du 1^{er} octobre 1999, le Sénat n'a pas désigné les trois nouveaux membres du Comité permanent R de sorte que, les quatre membres encore en fonction sont :

M. Jean-Claude Delepière, président
Mme Danielle Cailloux,
M. Gérald Vande Walle,
M. Jean-Louis Prignon.

Ceux-ci continuent à exercer leurs fonctions jusqu'à la nomination de leurs remplaçants.

LE GREFFIER DU COMITÉ PERMANENT R

Le Comité permanent R est assisté d'un greffier, lui aussi nommé par le Sénat. Il assure le secrétariat des réunions du Comité permanent R, en dresse les procès-verbaux et veille à l'expédition des pièces et à la conservation des archives. Le greffier est également responsable de la protection du secret de la documentation et des archives. Sa fonction est d'une durée indéterminée. Comme les membres du Comité permanent R, il doit être titulaire d'une habilitation de sécurité du niveau "très secret".

Le greffier actuel du Comité permanent R est Monsieur Wouter De Ridder, licencié en droit.

LE SERVICE D'ENQUÊTES DU COMITÉ PERMANENT R

Le cadre théorique actuel du Service d'enquêtes est de cinq personnes.

Le chef du Service d'enquêtes est nommé par le Comité permanent R pour un terme de cinq ans renouvelable une fois. Il doit être une personne d'expérience choisie parmi des magistrats, des membres ou des fonctionnaires des services de renseignements ou de police. Il doit connaître les langues française et néerlandaise. Le chef actuel du Service d'enquêtes est Monsieur Paul vander Straeten, premier substitut du procureur du Roi au parquet de Bruxelles.

Les membres du Service d'enquêtes sont nommés par le Comité permanent R sur proposition du Chef du Service d'enquêtes. Pour pouvoir être nommés, le chef et les membres du Service d'enquêtes doivent également être titulaires d'une habilitation de sécurité du niveau "très secret".

Les quatre membres actuels du Service d'enquêtes ont été nommés pour un terme renouvelable de cinq ans par détachement d'un service de police ou de renseignements.

LE PERSONNEL ADMINISTRATIF DU COMITE R

A la parution du présent rapport annuel, le cadre administratif du Comité permanent R se compose des collaborateurs suivants :

- S un comptable à titre statutaire;
- S une secrétaire à titre statutaire;
- S un employé à titre statutaire;
- S un employé à titre contractuel;
- S un réceptionniste à titre contractuel;
- S un chauffeur-technicien mis à disposition par les forces armées

Un autre militaire détaché des forces armées a pris sa pension dans le courant de l'année.

LES ACTIVITES DU COMITE PERMANENT R

Entre le 1^{er} août 1998 et le 31 août 1999, le Comité permanent R s'est réuni 52 fois.

Lors de ces réunions, des décisions ont été prises concernant les enquêtes, les textes du rapport annuel et la logistique.

De plus ont eu lieu également un grand nombre d'entretiens internes, de contacts avec les ministres compétents et leurs cabinets et, jusqu'à la dissolution des Chambres, des entretiens avec les Commissions de suivi parlementaire.

Pendant cette même période, seize nouvelles enquêtes ont été initiées, parmi lesquelles trois l'ont été à la demande du Parlement, une suite à une dénonciation anonyme, cinq suite à la plainte d'un particulier, six à l'initiative du Comité permanent R lui-même et une à l'initiative du Service d'enquêtes.

Le Service d'enquêtes a de plus apporté sa collaboration à deux enquêtes judiciaires.

Aucune enquête n'a été ouverte à la demande des ministres compétents.

Une enquête menée conjointement avec le Comité permanent P est encore en cours.

Les rapports des enquêtes de contrôle entièrement terminées sont repris sous le Titre II du présent rapport annuel.

LES MOYENS FINANCIERS DU COMITE PERMANENT R

Les moyens du Comité permanent R proviennent d'une dotation qui lui est accordée annuellement par le Parlement.

Depuis la loi du 1^{er} avril 1999, le greffier est responsable des comptes du Comité permanent R. Le règlement interne du Comité permanent R prévoit un contrôle interne des dépenses. Celui-ci est effectué par un des membre du Comité permanent R.

L'exécution du budget est placée sous la surveillance de la Cour des Comptes, qui établit chaque année un rapport à la demande de la Chambre des Représentants.

La dotation de l'année budgétaire 1998 se montait à 71.552.543 FB.
Sous réserve de l'approbation de la Chambre des Représentants, le solde positif de cette année se montait à 15.378.167 FB.

Le Parlement a accordé une dotation de 72.249.887 FB pour 1999.
Vraisemblablement, cet exercice présentera également un important boni à la clôture qui résulte en grande partie du fait que toutes les fonctions de membre du Comité permanent R et de membre de son personnel ne sont pas pourvues.

Un budget de 72.450.000 FB a été demandé pour l'année 2000.

ACTIVITES CONJOINTES AVEC LE COMITE PERMANENT P

Pendant la période de référence mentionnée au point 2, huit réunions conjointes ont eu lieu. Celles-ci avaient principalement pour objet une enquête commune spécifique. Cette enquête menée par une équipe d'investigation mixte, n'est pas encore clôturée.

Les deux institutions tombent sous l'application de la même loi organique, ont leur siège dans le même bâtiment, éditent des publications communes, leur personnel administratif a un statut similaire et elles ont un comité de sécurité commun.

C'est pourquoi une concertation permanente est indispensable entre les deux institutions et leurs greffiers.