COMITE PERMANENT DE CONTROLE

DES SERVICES DE RENSEIGNEMENTS

RAPPORT D'ACTIVITES

2003

Rue de la Loi 52 - 1040 Bruxelles

Tél 02/286.28.11 -- Fax 02/286.29.99

www.comiteri.be - e-mail : info@comiteri.be

TABLE DES MATIERES

TITRE 1 : INTRODUCTION

INTRODUCTION GENERALE

1. PREAMBULE

Le présent rapport annuel d'activités 2003 marque les dix années révolues d'existence du Comité permanent R institué par la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements. Les Comités permanents P et R ont débuté leurs activités en juin 1993.

A l'occasion de ce rapport, le Comité permanent R en revient à une présentation plus exhaustive des enquêtes finalisées au cours de l'année 2003 et qui, en application des articles 33 al. 3 et 35 de la loi précitée ont été transmises à la Chambre des représentants, au Sénat ainsi qu'aux ministres compétents de la Justice et de la Défense nationale.

Le rapport général d'activités précédent relatif à la période 2002 avait en effet été présenté, sous une forme plus expurgée compte tenu du dépôt de ce document à un moment où, pour cause d'élections législatives, le Parlement était dissous.

En tout état de cause, le Comité permanent R reste conscient de la difficulté de trouver le juste équilibre entre d'une part, les impératifs légaux du respect de la vie privée et les règles de classification auxquels est soumise sa double mission de contrôle[1] et d'autre part, le rôle qui est également le sien de donner à la société ainsi qu'aux autorités civiles la plus grande lisibilité[2] possible concernant une matière délicate, par essence peu accessible et parfois aussi sujette à une certaine défiance.

Le risque d'atteinte au bon fonctionnement des services de renseignement et de sécurité, y compris dans le contexte des relations internationales, est également à mettre dans la balance au cours de cette recherche du juste milieu. Cette démarche constitue une préoccupation importante et permanente du Comité permanent R.

Dans la manière de faire rapport, et outre ces aspects, le Comité permanent R doit tenir compte également et d'une façon raisonnable et appropriée, des sensibilités de toute nature qui se rencontrent à différents échelons de la société, face à certaines problématiques.

L'exercice est d'autant plus difficile que l'activité du renseignement a pour finalité d'évaluer et de communiquer aux autorités décisionnelles l'existence ainsi que le degré de gravité des « menaces » définies par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. La tâche des services de renseignement n'est donc pas de rapporter des faits avérés ou prouvés selon la procédure judiciaire. Ceci constitue d'ailleurs une des différences fondamentales avec les missions des services de police.

---

1 Elle porte sur la protection des droits que la constitution et la loi confèrent aux personnes ainsi que sur la coordination et l'efficacité des services de renseignements et de sécurité

2 L'article 37 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement prévoit que : « *Après avoir recueilli l'avis des ministres compétents, le Comité permanent R décide, dans un délai d'un mois à compter de la demande d'avis, de rendre public tout ou partie de ses rapports et conclusion, selon les modalités qu'il détermine …* »

Le fait de tenir compte de ces divers éléments ne peut toutefois exclure pour le Comité permanent R la prise entière de ses responsabilités dans la façon dont il doit rigoureusement faire rapport à plusieurs niveaux et le cas échéant sous des formes différentes[3] (au pouvoir législatif, au pouvoir exécutif, à l'opinion publique), de son contrôle sur les activités et les méthodes des services de renseignement.

Il est important de rappeler ici que cette prise de responsabilité se réalise de manière collégiale par le Comité permanent R composé, à l'instar du Parlement, de manière pluraliste. Le législateur a ainsi voulu éviter que des influences extérieures, préjudiciables au bon fonctionnement de l'organe de contrôle puissent s'exercer.

En tout état de cause, il est clair pour le Comité permanent R que les constatations, questions, conclusions et recommandations qui résultent des enquêtes de contrôle publiées dans le présent rapport ne sont que des étapes qui se veulent être exclusivement une contribution constructive au maintien et au renforcement de l'ordre constitutionnel et démocratique.

Dans le début de ce 21ème siècle marqué par l'augmentation de menaces nationales et internationales multiformes comme celles des extrémismes, des organisations criminelles et du terrorisme, le contrôle parlementaire des services de police et de renseignement auquel le Comité permanent R participe depuis 10 ans, s'inscrit donc, plus que jamais, dans la volonté exprimée par le législateur dès les premières dispositions de la loi organique du 30 novembre 1998 organique des services de renseignement et de sécurité, de voir ces services, veiller dans l'exercice de leurs missions « au respect » des droits et libertés individuelles et « contribuer à leur protection, ainsi qu'au développement démocratique de la société » (art.2 – 2ème alinéa).

Ce contexte légal n'est pas en opposition avec le souhait du Comité permanent R, également fondé sur sa finalité légale, de contribuer à optimaliser l'efficacité des services de renseignement. Il est clair que de nos jours, ceux-ci ont un rôle de première ligne à jouer dans la lutte contre les menaces pour la démocratie.

2. GENERALITES

2.1. Les enquêtes de contrôle

Du 1er janvier au 31 décembre 2003, le Comité permanent de contrôle des services de renseignement et son Service d'enquêtes ont eu en traitement un total de 36 enquêtes, dont 21 ont été ouvertes au cours de la même période. Parmi ces dernières enquêtes, 9 ont été ouvertes à l'initiative du Comité permanent R, 9 à la suite de plaintes de particuliers, 2 à l'initiative du Service d'enquêtes et 1 à l'initiative des deux Comités permanents P et R.

Ces enquêtes concernent pour 12 d'entre elles uniquement la Sûreté de l'Etat et pour 3 d'entre elles, uniquement le Service général du Renseignement et de la sécurité des forces armées. Les 6 enquêtes restantes sont relatives à des matières qui relèvent de la compétence des deux services. Neuf des 12 enquêtes relatives à la Sûreté de l'Etat ont été ouvertes à la suite de plaintes de particuliers ou de membres de ce service.

[3] Notamment en fonction des règles de classification

A la date de clôture du présent rapport, 18 enquêtes de contrôle sont toujours en cours d'exécution, soit que des devoirs complémentaires sont encore à exécuter par le Service d'enquêtes, soit que celui-ci a transmis les résultats de ses investigations au Comité permanent R qui prépare un rapport destiné, comme l'article 33, 3ème alinéa de la loi organique de contrôle le prévoit, aux ministres concernés ainsi qu'à la Commission sénatoriale de suivi.

Parmi les enquêtes ouvertes en 2003, il convient de souligner certains des sujets qui ont retenu l'attention du Comité permanent R. Les résultats de ces enquêtes feront l'objet de rapports au cours de l'année 2004.

En premier lieu, et suite à des constatations ponctuelles du Service d'enquêtes du Comité permanent R (voir point 2.2), ce service a pris l'initiative, conformément à l'article 40 de la loi organique du 18 juillet 1991 relative au contrôle des services de police et de renseignement, d'ouvrir une enquête sur « *la manière dont la Sûreté de l'Etat et le Service général de renseignement et de sécurité contrôlent l'accès au Registre National afin de prévenir ou de détecter des abus éventuels dans le chef de leurs collaborateurs ».*

En second lieu, dans le cadre de la menace terroriste, le Comité permanent R a chargé son Service d'enquêtes de recueillir les informations nécessaires « *sur la manière dont les services de renseignement envisagent leur rôle dans le contexte des menaces d'emploi de moyens nucléaires, biologiques et chimiques dans les actions terroristes ».*

En troisième lieu, le Comité permanent R s'intéresse à une des nouvelles compétences légales des services de renseignement (articles 7 et 8 de la loi du 30 novembre 1998 - loi organique des services de renseignement et de sécurité) dans le cadre d'une enquête de contrôle sur : « *la manière dont les services de renseignement belges fonctionnent et collaborent dans le cadre de leur nouvelle mission légale concernant les menaces des organisations criminelles ».*

Enfin, les deux comités P et R ont entamé une enquête commune sur « *la coordination entre les différents services de police et de renseignement dans la lutte contre le terrorisme ».*

Les rapports d'enquêtes déjà transmis aux ministres de la Justice et de la Défense nationale ainsi qu'au Parlement sont, quant à eux, dans leur version publique, repris sous le titre II du présent rapport général d'activités 2003. Ils mentionnent le cas échéant, les observations, commentaires et avis des ministres compétents.

2.2. Les enquêtes judiciaires

L'article 40 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement prévoit que le Service d'enquêtes du comité permanent R « d'initiative ou sur réquisition du procureur du Roi ou du juge d'instruction compétent, effectue, en concurrence avec les autres officiers et agents de police judiciaire et même avec un droit de prévention sur ceux-ci, les enquêtes sur les crimes et délits à charge des membres des services de renseignements.»

En ce qui concerne cette compétence particulière, que le Comité permanent R en tant que tel ne partage pas, le Service d'enquêtes est intervenu dans le cadre de 9 affaires judiciaires, dont 4 dossiers faisant l'objet d'une instruction. Outre Bruxelles, les arrondissements judiciaires de Termonde, Hasselt et Verviers sont concernés. Au total, 44 procès-verbaux ont été rédigés et une personne a été mise à la disposition du juge d'instruction qui a délivré mandat d'arrêt.

Ces enquêtes qui augmentent en nombre par rapport aux années précédentes, mettent en évidence l'existence de problèmes auxquels les dimensions judiciaires apportent des éclairages nouveaux et plus concrets qui sont de nature à susciter l'intervention du Comité permanent R dans le contexte de sa mission d'organe de contrôle externe.

C'est ainsi que, faisant suite à plusieurs de ces enquêtes judiciaires, le Comité permanent R a ouvert de son côté des enquêtes de contrôle sur la base des informations auxquelles il a eu accès, avec l'autorisation des autorités judiciaires. La plupart de ces enquêtes sont toujours en cours, à l'exception d'une affaire, dont le rapport public est repris en page 215 du présent document.

Les dossiers encore en traitement sont liés à des sujets de premier ordre comme l'application de la loi sur la classification et le respect de la vie privée.

Le Comité permanent R fera rapport dans le courant de l'année 2004 sur deux dossiers particulièrement importants qui touchent ces domaines sensibles. Le premier de ces dossiers a pour objet le seul cas actuellement connu du Comité permanent R depuis l'entrée en vigueur de la loi relative à la classification et aux habilitations de sécurité, de divulgation illicite d'un document classifié.

Le second dossier judiciaire a justifié l'ouverture d'une enquête plus générale pour vérifier les mesures mises en place par les deux services de renseignement pour surveiller l'accès et la consultation par leurs membres des données du Registre national, afin de prévenir ou de détecter tout abus éventuel attentatoire au respect de la vie privée.

2.3. Les activités d'organe de recours du Comité permanent R

La loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité a institué le Comité permanent R comme organe de recours. Cette disposition législative est entrée en vigueur le 1er juin 2000.

Des évaluations de cette activité ont déjà fait l'objet de communications dans les rapports d'activités 2000 (p. 17 à 25), 2001 (p. 11 à 13) et 2002 (p. 37 à 44).

Au cours de l'exercice 2003, onze dossiers de recours ont été instruits. Trois de ces recours concernaient des procédures initiées par l'Autorité nationale de sécurité, les huit autres étant relatifs à des décisions prises par le SGRS agissant en tant qu'autorité de sécurité pour le personnel de la Défense nationale.

Aucun recours n'a été introduit pour des procédures similaires concernant la Sûreté de l'État.

Dans deux cas, la décision de l'autorité de sécurité a été modifiée et l'habilitation initialement refusée a été octroyée avec une limitation dans le temps.

Dans six autres dossiers, le recours a été déclaré recevable et non fondé. Dans deux cas, le recours a été déclaré sans objet. Dans un cas, il a été déclaré irrecevable compte tenu du dépassement du délai légal d'introduction de l'action.

Depuis l'entrée en vigueur de la loi, l'évolution du nombre de recours se présente de la manière suivante :

Année	2ème semestre. 2000	2001	2002	2003	1er trimestre 2004	Total
Nombre de recours	19	17	17	11	3	67

Comme cela avait déjà été constaté lors de l'exercice précédent, le nombre de recours continue à décroître en 2003. Les chiffres du premier trimestre 2004, s'ils devaient se maintenir par la suite, confirmeraient la moyenne actuelle d'un recours par mois.

Le Comité permanent R continue à être surpris par le nombre réduit de recours et par le fait que la quasi totalité de ceux-ci sont introduits par des militaires contre des décisions du SGRS agissant comme autorité de sécurité à l'égard du personnel de la Défense nationale (cf rapport général d'activités 2002 pp 37 et 38).

Sur la base de cette constatation, le Comité permanent R a donc décidé d'activer une enquête générale de contrôle sur la manière dont les Services de renseignement belges appliquaient la législation en matière d'habilitation de sécurité. Cette enquête devrait permettre au Comité permanent R de disposer, si elles existent, de statistiques globales concernant le nombre d'enquêtes de sécurité, le nombre de décisions de refus ou de retrait et de tirer des conclusions sur la signification de la quantité réduite des recours.

Le Comité permanent R rappelle, en effet, que chaque année ce sont des milliers de dossiers d'habilitation qui sont traités et que le résultat de ce traitement influence directement la situation professionnelle des intéressés. Le refus ou la perte d'une habilitation de sécurité signifie la plupart du temps la perte d'un emploi, d'un contrat ou d'une fonction intéressante.

Les conclusions de l'enquête en cours devront donc porter fondamentalement sur les éléments qui conditionnent la recherche du meilleur équilibre possible entre les intérêts de la personne qu'elle soit physique ou morale, et ceux de la sécurité générale.

A l'occasion des décisions individuelles rendues en 2003, le Comité permanent R a eu l'occasion de rappeler la spécificité des enquêtes de sécurité et donc aussi celle du recours qui y est associé : évaluer la capacité d'une personne ayant accès à des informations classifiées à n'en faire usage qu'en exécution stricte des règles de sécurité. Il est donc évident qu' aussi bien les autorités de sécurité que l'organe de recours se trouvent dans un contexte d'appréciation à la fois beaucoup plus large et plus délicat que dans n'importe quelle autre matière.

C'est ainsi que des faits et des comportements propres au requérant ou à son environnement familial ou social, peuvent et doivent être pris en considération par les autorités de sécurité pour évaluer son degré de fiabilité, même si ces faits ou comportements ne doivent pas nécessairement faire ou avoir fait l'objet d'une procédure judiciaire ou disciplinaire.

L'octroi ou le maintien d'une habilitation de sécurité dépend donc d'une évaluation comportant une certaine part de subjectivité et du moment où celle-ci est effectuée.

En ce qui concerne le critère de temporalité, l'organe de recours a constaté, comme il l'avait déjà fait précédemment, que dans certains cas des éléments défavorables d'appréciation datant d'une période située avant l'engagement d'une personne dans les forces armées se révélaient ou resurgissaient à l'occasion d'une enquête de sécurité dans le cadre d'une procédure d'habilitation (cf. rapport général d'activités 2000 - p. 23).

Le Comité permanent R rappelle qu'il préconisait à ce sujet que la problématique de sécurité soit déjà intégrée dans la phase de recrutement pour informer complètement les candidats de l'influence ultérieure possible de certains paramètres personnels sur les exigences de sécurité liées à certaines fonctions au sein des forces armées.

Enfin, le Comité permanent R tient à souligner que dans le cadre de sa mission d'organe de recours, il n' a jusqu'à ce jour jamais été confronté à un recours introduit par une personne morale. Au delà de l'aspect des recours, le Comité permanent R attire ici l'attention sur la problématique de la sécurité des entreprises sensibles ou stratégiques, et des personnes qui y travaillent (voir à ce sujet infra « Le rapport sur l'intérêt qu'ont porté les services de renseignements à un vol de données sensibles commis dans une société commerciale belge fournissant des produits et services de haute technologie » p. 204 et le « Rapport de l'enquête de contrôle sur l'intervention des services de renseignement dans un cas de disparition inquiétante d'une personne travaillant dans un secteur lié à la Défense nationale » p. 210)

Dans le cadre d'une bonne prévention des menaces, le Comité permanent R estime qu'en matière de sécurité et donc notamment d'habilitations, l'accent devrait être mis sur la qualité de l 'évaluation des risques et des enquêtes de sécurité plutôt que sur une augmentation de la quantité des postes et fonctions soumis à habilitation légale. Le Comité permanent R a déjà concrètement fait part de cette réflexion en ce qui concerne les habilitations de sécurité du personnel militaire.

Pour conclure, le Comité permanent R fait observer que le nombre réduit des recours introduits n'enlève rien à l'importance de cette procédure, aussi bien au niveau de la protection de droits des personnes qu'au niveau des exigences du droit constitutionnel et du droit européen.

Cette compétence apporte d'autre part au Comité permanent R une vue concrète sur un domaine lié au monde du renseignement susceptible d'alimenter utilement sa réflexion ainsi que sa démarche dans sa mission de contrôle.

3. L'IMPORTANCE GENERALE DE LA PROBLEMATIQUE DE L'INFORMATION

S'il y a un risque de dysfonctionnement qui est clairement et incontestablement apparu dans un passé encore récent à l'occasion de diverses enquêtes parlementaires, c'est bien celui de la rétention d'informations.

Certes, les modifications légales sont le premier moyen de répondre à ce type de dysfonctionnement grave. Le Comité permanent R se pose toutefois la question de savoir si cette approche est suffisante pour éviter, dans l'avenir, ce genre de problème avec un certain degré de garantie.

Il ne s'agit plus ici de la forme de la coopération entre services ou de la communication de ceux-ci avec les autorités, mais du contenu même de cette coopération ou de cette communication.

Cette attitude qui consiste pour certains à considérer qu'une information ne peut être partagée parce qu'elle peut rencontrer un intérêt propre qu'il soit personnel ou de service, doit être fermement combattue.

Il convient en effet de rappeler :

- que dans des domaines hautement concernés par la protection de la démocratie et des citoyens, l'information - même si elle doit être dans certains cas protégée[4] -n'est la propriété de personne ;

- que cette information doit être mise à la disposition des autorités et des personnes à qui elle doit être légitimement utile ; ce qui n'exclut nullement que cette communication, lorsqu'il s'agit de données à caractère personnel, réponde à des conditions légales strictes (cf. l'enquête de contrôle et la plainte concernant Madame S. Collier p. 137 et l'avis du Comité permanent R concernant le cadre juridique dans lequel la Sûreté de l'Etat et le SGRS peuvent procéder à des vérifications de sécurité sur des personnes et transmettre des avis et informations à caractère personnel aux autorités p. 263.).

- que la loi organique qui définit les missions de la Sûreté de l'Etat et du SGR, consacre le caractère obligatoire de cette communication des renseignements aux instances et personnes compétentes et/ou concernées par une menace ;

- que cette obligation est proportionnelle à la gravité de la menace et qu'il ne peut y être dérogé que si des motifs de protection des personnes ou de classification apparaissent supérieurs à l'importance de la menace ;

- que l'existence d'une obligation implique celle d'une responsabilité qui doit pouvoir être évaluée et éventuellement sanctionnée au sens large.

La logique qui relie les éléments précités est illustrée par l'article 44 de la loi sur la fonction de police qui édicte la communication obligatoire des informations à la banque nationale de données. Cette obligation est sanctionnée pénalement

Ce type de disposition comme celle de l'article 19 de la loi organique des services de renseignements et de sécurité du 30 novembre 1998 pré-rappelé, pose la question du contrôle de la communication des informations utiles aux bénéficiaires.

En ce qui concerne les services de renseignements, celui-ci peut-être effectué par le Comité permanent R au travers du contrôle de l'efficacité et de la coordination de ces services (la Sûreté de l'Etat et le SGR).

Les mécanismes de concertation du Comité permanent R avec aussi bien les ministres de tutelle des deux services de renseignement belges qu'avec les commissions parlementaires de suivi, prévus par la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement, sont susceptibles de donner à ce contrôle la profondeur voulue et de développer ainsi une nouvelle culture et une nouvelle perception du renseignement davantage axées sur la prévention des menaces à long terme.

Le Comité permanent R pense également qu'une concertation avec le Comité ministériel du renseignement et avec le Collège du renseignement serait de nature à contribuer à l'amélioration du processus de collaboration et de coordination des services.

[4] Loi relative à la classification et aux habilitations de sécurité du 11 décembre 1998 (MB du 7 mai 1999)

Dans ce même ordre d'idée, le Comité permanent R avait, dans son rapport général d'activités 2001 (p. 206-207), établit une liste des informations indispensables dont le Comité estimait devoir disposer afin d'accomplir sa mission plus efficacement. Parmi-celles-ci, étaient reprises les mesures visant les services de renseignement prises par le Comité ministériel du renseignement et de la sécurité ou par les ministres compétents.

Etaient concernés également, les arrêtes royaux, ministériels et réglementaires pris en exécution de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et qui, le cas échéant, ne font pas l'objet d'une publication au Moniteur belge.

Dans le cadre du même rapport (cf. p. 201-202), le Comité permanent R soulignait qu'à sa connaissance, *« les mesures d'application suivantes de la loi du 30 novembre 1998 n'avaient pas encore été prises, bien qu'il existe des protocoles d'accords entre les services concernés.*

C'est ainsi que conformément à l'article 20 §3 de la loi du 30 novembre 1998 organique précitée, le Comité ministériel du renseignement et de la sécurité devrait :

- *définir les conditions de la communication prévue à l'article 19, alinéa 1er, c'est-à-dire la communication de renseignements aux ministres et autorités administratives et judiciaires concernés, aux services de police et à toutes les instances et personnes compétentes ;*

- *définir les conditions de la coopération prévue à l'article 20, §1er c'est-à-dire la collaboration avec les autres services de renseignement belges et étrangers, avec les autorités administratives et judiciaires. »*

Le Comité permanent R rappelle également « les propositions de mesures législatives et autres à prendre en matière de renseignement » qu'il avait présentées à la demande de la commission permanente du Sénat chargée du suivi du Comité permanent R (rapport général d'activités 2001- p. 200 e.s.)

C'est dans ce contexte également que le Comité permanent R avait plaidé pour la création en Belgique d'un poste de coordinateur fédéral du renseignement (voir infra point 4.3).

Le Comité permanent R renvoie à ces propositions qu'il réitère en insistant sur celles qui devraient permettre de répondre aux exigences impérieuses d'une meilleure communication des informations et de leur coordination.

4. L'EFFICACITE ET LA COORDINATION DES SERVICES DE RENSEIGNEMENT

Pour un service de renseignement, l'efficacité est en grande partie déterminée par trois éléments : l'information qui peut être recueillie, la manière dont cette information est traitée et analysée et enfin la manière dont le renseignement est communiqué.

4.1. Le recueil de l'information

4.1.1. Les dispositions légales

Seuls, les articles 14 à 18 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité sont consacrés au recueil des données par les services de renseignement.

Ces dispositions sont de nature très générale puisqu'elles évoquent principalement l'échange d'informations entre les services de renseignement et d'autres autorités publiques, le principe de la communication aux services de renseignement des données provenant de registres comme ceux de la population et des étrangers, la référence aux dispositions de la loi du 8 décembre 1992 relative à la protection de la vie privée et la possibilité pour les services de renseignement et de sécurité d'avoir recours à des « sources humaines ».

Pour le surplus, l'article 20 de la même loi fait obligation aux services « d'assurer entre eux une coopération mutuelle aussi efficace que possible » et d'assurer également « une collaboration avec les services de renseignement et de sécurité étrangers ».

En ce qui concerne les moyens techniques de recueil de l'information, le Comité permanent R rappelle que seul à ce jour, le SGRS peut légalement, dans certaines conditions, recueillir des informations par le recours à des interceptions de communications émises à l'étranger (voir les articles 44, 44 bis et 44 ter de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité telle qu'elle a été modifiée par la loi du 3 avril 2003 – M.B. 12-05-2003 – p.25.376).

Incidemment, il faut mentionner à ce sujet que l'article 4 de la loi du 3 avril 2003, modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'article 259 bis du code pénal, a introduit un nouvel article 44 bis qui attribue le contrôle de ces interceptions de communications au Comité permanent R (M.B. du 12-05-2003 p. 25376).

Enfin, il faut signaler également les dispositions légales relatives à la classification et aux habilitations de sécurité[5] qui s'appliquent dans certaines conditions aux informations recueillies par les services de renseignement.

4.1.2. Synthèse des constatations du Comité permanent R en la matière

Dans le domaine du recueil des informations, le Comité permanent R a toujours distingué les moyens législatifs, techniques et humains. En ce qui concerne le premier de ces aspects, le Comité permanent R a recommandé à plusieurs reprises, dans ses rapports d'activités précédents, que l'on accorde aux services de renseignement et, principalement à la Sûreté de l'Etat , la possibilité de pratiquer sous contrôle, des interceptions administratives de communication (Cf.. rapport général d'activités 2001 – Document de travail relatif aux conditions d'octroi à la Sûreté de l'Etat et au SGR de l'autorisation éventuelle de procéder à des interceptions de sécurité (p. 208)).
Le Comité permanent R a notamment déjà attiré l'attention sur le fait que *« dans le concert international, l'absence de législation belge en matière d'écoutes de sécurité place la Sûreté de l'Etat sur un plan d'infériorité par rapport aux services étrangers qui disposent d'un tel moyen d'action ».*

[5] Loi du 11 décembre 1998

D'une manière plus générale, le Comité permanent R a souligné dans son rapport d'activités 2001 « que l'utilisation de techniques spéciales de recherche intrusives pour la vie privée (écoutes, filatures, informateurs, …) par les services de renseignement doit faire l'objet de normes légales prévoyant le respect des principes de subsidiarité et de proportionnalité. De telles mesures sont indispensables aussi bien du point de vue de l'efficacité des services que de celui de la protection des droits des citoyens » (rapport général d'activités 2001- pp. 193-194).

Le Comité permanent R estime qu'une réglementation légale est aujourd'hui, plus que jamais indispensable pour les services de renseignement, alors que de telles dispositions existent pour les services de police[6] en conformité notamment avec les exigences de la Convention européenne de sauvegarde des Droits de l'Homme et des libertés fondamentales (cf. pour les services de police - la loi du 6 janvier 2003 concernant les méthodes particulières de recherche et quelques autres méthodes d'enquête).

En ce qui concerne les moyens techniques de recueil de l'information, et outre ce qui est rappelé ci-dessus concernant l'aspect de la légalité, le Comité permanent R a souligné à plusieurs reprises que de toutes les méthodes employées, l'utilisation d'informateurs était sans doute la plus essentielle, mais en même temps la plus délicate tant du point de vue de l'efficacité que du respect des libertés et droits fondamentaux (rapport général d'activités 1999 – p.9).

Les événements dramatiques des derniers temps en matière de terrorisme ont démontré l'importance fondamentale de cette source de renseignements en corrélation avec d'autres sources d'informations, comme les sources ouvertes et l'utilisation de moyens technologiques modernes.

A plusieurs reprises au cours des années précédentes, le Comité permanent R a mis en évidence le fait qu'il n'existait pas véritablement de règles précises pour encadrer l'utilisation de ce type de sources humaines.

Les services de renseignement ont toutefois toujours témoigné une certaine réticence à ce que cette matière soit réglementée par voie légale.

Dans son rapport de 2001, le Comité permanent R rappelait toutefois que « *si des notes internes existent, dans la pratique, la manière de traiter les informateurs semble le plus souvent laissée à l'appréciation ponctuelle des agents des services extérieurs ».*

Sans pouvoir entrer dans les détails de l'affaire, le Comité permanent R illustre aujourd'hui ce propos en se référant à la condamnation pénale récente d'un membre d'un service de renseignement qui dans le cadre de la manipulation d'un informateur avait, d'initiative personnelle, dans le but de s'attirer la confiance d'une source, émis un chèque sans provision d'un montant considérable.

Dans une mesure qui n'est absolument pas comparable quant aux faits et quant aux conséquences, le rapport d'enquête suite à la plainte d'un particulier relatif au comportement d'agents de la Sûreté de l'Etat repris en page 245 du présent document illustre néanmoins une nouvelle fois cette thématique sensible des informateurs et la nécessité pour le Comité permanent R de disposer d'un encadrement légal et réglementaire rigoureux aussi bien pour assurer l'efficacité et la coordination optimales des services dans cette matière, que pour assurer également la protection des droits des personnes et des fonctionnaires impliqués dans de telles activités.

[6] voir aussi la législation néerlandaise du 7 février 2002 "contenant des dispositions concernant les services de renseignement et de sécurité ainsi que la modification de certaines lois" (art. 12 es.).

Le Comité permanent R relève à ce sujet une autre question qu'il lui semble urgente d'aborder en cette matière : celle de la coordination de la gestion des informateurs entre les différents services chargés dans les limites de leurs compétences respectives, de la lutte contre le terrorisme.

De l'avis du Comité permanent R, le système actuel très cloisonné dans la pratique, aussi bien au sein des services qu'entre ceux-ci, ne semble pas permettre d'identifier les informateurs qui travailleraient en même temps pour la Sûreté de l'Etat, le SGRS et la police. Le Comité permanent R craint que dans ces conditions et dans la période internationale troublée que nous connaissons, des manipulations de toute nature, dans cette sphère d'activités communes des services de sécurité, représentent un risque réel à prendre en considération par les autorités.

Déjà dans son rapport d'activités 1997, le Comité permanent R indiquait dans la conclusion générale d'une enquête de contrôle sur l'utilisation d'informateurs par la Sûreté de l'Etat et le SGRS que : *la collaboration entre services de police et services de renseignement à l'occasion des sujets comme la criminalité organisée, le terrorisme, etc … devra faire l'objet d'une attention particulière*.

Le risque existe en effet, que dans les domaines mentionnés ci-dessus, la différence entre informateurs des services de police et les informateurs des services de renseignement s'estompe et que des deux types de services doivent faire face à des problèmes comparables (rapport général d'activités 1997 – p.163) .

D'autres domaines connexes touchant également au recueil de l'information ont aussi retenu dans un passé récent l'intérêt du Comité permanent R. C'est ainsi que celui-ci rappelle la problématique des systèmes globaux d'interception de communications de type « Echelon » (voir rapport général d'activités 2000 - Rapport de synthèse sur la manière dont les services belges de renseignement réagissent face à l'éventualité d'un réseau « Echelon » d'interception de communications en Belgique – p.29 et suivantes).

A cette occasion, le Comité permanent R avait mis en exergue la menace que les possibilités technologiques actuelles d'interception de communications étaient susceptibles de présenter si elles étaient, par exemple, utilisées par des organisations criminelles ou terroristes pour recueillir des informations confidentielles sur la sécurité et le potentiel scientifique et économique du pays. Le Comité permanent R avait relevé dans le même ordre d'idée en 2001, que depuis plusieurs années le SGRS préconisait une politique de sécurisation de l'information concertée au niveau fédéral (voir rapport général d'activités 2001 - p.184).

A la suite de cette constatation, le Comité permanent R avait émis des recommandations qui visaient e.a. la mise en place d'une politique globale et centralisée de sécurité de l'information, ainsi que l'instauration d'un service chargé d'apporter une solution à l'ensemble de cette problématique.

Le Comité permanent R observe également que cette technique d'interception globale des communications, considérée il y a quelques années encore par certains comme fantaisiste, a été entre-temps reconnue comme une réalité incontournable à laquelle les services de renseignement ont de plus en plus souvent recours.

Plusieurs dossiers d'enquêtes du Comité permanent R ont souligné de la même manière la nécessité d'une protection des systèmes d'information et de communication, face aux faiblesses des réseaux de transmission résultant non seulement des développements technologiques, mais aussi de la libéralisation de ces marchés. Même des opérateurs reconnus ont, dans ces conditions, des difficultés à garantir la sécurité des moyens de télécommunications.

Trois ans après avoir émis ces recommandations, le Comité permanent R s'interroge d'autant plus sur l'évolution qu'a connu ce domaine, alors qu'il s'est penché en 2003 sur l'émergence du rôle des services de renseignement privés dans notre pays dans le cadre d'une enquête dont la version publique du rapport est reprise en page 24 du présent document.

Le problème du contrôle posé par cette sphère privée du renseignement reste entier, notamment à l'égard des techniques de recueil de l'information et de leur légalité.

En ce qui concerne l'aspect des moyens humains, le Comité permanent R a plaidé à de nombreuses reprises pour que les services de renseignement belges disposent des ressources humaines nécessaires et qualifiées.

Le Comité permanent R a également constaté en 2001 (rapport général d'activités 2001 – p. 186) qu'à l'heure actuelle les compétences légales de la Sûreté de l'Etat étaient limitées à l'intérieur du territoire national, ce service ne disposant d'aucune représentation à l'étranger.

Le Comité permanent R estime que ce problème devrait être examiné. La question se pose, en effet, de savoir s'il est utile que la Sûreté de l'Etat dispose de ses propres représentants à l'étranger, à côté des attachés militaires et des officiers de liaison de la police fédérale. Ne va-t-on pas ainsi créer un problème supplémentaire et ne vaudrait-il pas mieux trouver la solution dans un meilleur partage de l'information ? On ne peut d'ailleurs pas nier qu'un officier de liaison de la police fédérale traite également pour une part non négligeable des informations autres que policières. Vu sous cet angle, on pourrait considérer qu'il y a déjà dans le domaine du renseignement civil une présence à l'étranger.

4.2. Le traitement de l'information

L'audit de la Sûreté de l'Etat, durant la troisième phase (voir page 148 du présent rapport général d'activités) a clairement montré qu'il n'y avait pas de lacune importante dans le recueil de l'information, mais qu'une maîtrise insuffisante du flux interne de cette information pouvait constituer un handicap pour la production utile d'une analyse de qualité.

Le Comité permanent R attend les directives qui seront prises en la matière par la hiérarchie de la Sûreté de l'Etat. Il en suivra le développement.

D'une manière générale, le Comité permanent R a relevé au cours de périodes antérieures et à l'occasion d'enquêtes de contrôle touchant des domaines divers de la compétence des services de renseignement, que c'était surtout au niveau du traitement des informations que se situait un des points clefs du cycle du renseignement devant mener à la production d'analyses stratégiques pertinentes délivrées en temps utile aux autorités décisionnelles compétentes.

C'est ainsi que dans son rapport d'activités 2001, le Comité permanent R posait les deux questions suivantes :

« *A de nombreuses reprises, le Comité permanent R s'est demandé, notamment en ce qui concerne le renseignement civil, si les analyses transmises aux diverses autorités répondaient bien toujours qualitativement aux attentes des destinataires ? A l'inverse, on pourrait également se demander si les services de renseignement savent toujours bien ce que les décideurs attendent d'eux ? » (Rapport général d'activités 2001 – p. 8).*

Le Comité permanent R estime que ces questions sont de celles qui doivent continuellement être prises en compte, à tout niveau, afin d'évaluer et d'améliorer la qualité du renseignement stratégique. Au cours de l'exercice écoulé le Comité permanent R a pu constater qu'elles sont plus que jamais d'actualité.

A titre d 'exemple, le Comité permanent R se réfère aux conclusions du rapport de l'enquête sur : « *la manière dont les services de renseignement ont traité et diffusé des informations relatives à des affaires de fraude aux visas et autres documents favorisant la traite des êtres humains vers la Belgique »* (voir page 164 du présent rapport général d'activités), dans lesquelles il constate et regrette que la Sûreté de l'Etat n'ait pas été en état de produire une synthèse et une analyse globale des pratiques dénoncées par le Centre pour l'égalité des chances dans son rapport de mai 2001, à savoir : *« l'infiltration des milieux officiels par des milieux criminels organisés afin d'obtenir des faux visas et documents permettant le séjour en Belgique ».*

Pour ce qui est de l'autre aspect des questions posées, à savoir à quelles attentes des autorités les services doivent-ils répondre, le Comité permanent R rappelle à nouveau la problématique de la protection du potentiel scientifique et économique du pays, pour laquelle la Sûreté de l'Etat n'a toujours pas reçu les directives du Comité ministériel du renseignement (Voir à ce sujet le rapport concernant « la protection du potentiel scientifique et économique du pays : le rôle des services de renseignements privés et publics » - « Le rapport de l'enquête de contrôle sur les éventuelles activités de la Sûreté de l'État concernant la protection du potentiel économique et scientifique lors de la faillite de la firme KPNQwest », et « Le rapport sur la manière dont la Sûreté de l'État a fonctionné relativement à une information éventuelle dans le dossier Ford Genk. dans le cadre de sa mission de protection du potentiel scientifique et économique », p. 227 du présent document).

4.3. La communication du renseignement et sa coordination

Les attentats du 11 septembre 2001 et du 11 mars 2004, ainsi que le conflit irakien, ont soulevé, à plusieurs reprises, le problème crucial d'une bonne communication aux autorités, des renseignements concernant la menace.

La Belgique n'échappe pas à cette problématique. Le Comité permanent R estime que des améliorations doivent être apportées à ce niveau. Dans son rapport annuel 2001 (p.29), le Comité permanent R revenait à ce propos sur une recommandation qu'il avait déjà formulée en 1995, de la mise en place d'un coordinateur du renseignement *« qui disposerait d'une vue d'ensemble de la production des services opérationnels. Son rôle serait notamment de recevoir les rapports des deux services de renseignements (SE et SGR) dans les domaines jugés prioritaires par le Comité ministériel du renseignement et des autres ministres et autorités concernées… ».*

Dans son rapport de l'enquête relative à la manière dont la Sûreté de l'Etat a géré l'information au sujet de l'ETA (Cf. rapport général d'activités 2001 - p. 36 à 40), le Comité permanent R constatait aussi « *qu'en tenant compte des diverses autorités qui sont concernées et qui n'ont sans doute pas les mêmes intérêts et les mêmes priorités au même moment, … se posait également la question de savoir si nonobstant l'existence de structures comme le Comité ministériel du renseignement et le Collège du renseignement, il existait une véritable coordination du renseignement en Belgique ?*

Qui décide, par exemple, d'une manière générale des limites qui ne peuvent être dépassées dans ses actions, par une organisation qui, sans être « terroriste » sur le territoire national ou éventuellement même sur celui de l'Union européenne, dispose d'une structure susceptible d'intégrer à la fois des activités légales et des activités illicites et clandestines ? »

La question d'une très grande complexité, il est vrai, semblait primordiale à l'époque. Elle reste toujours d'une actualité sensible.

Cette problématique amène incidemment le Comité permanent R à envisager la piste de réflexion suivante : les services de renseignement, les organes de coordination (ou encore mieux, un coordinateur) n'ont-ils pas également une sorte de « mission pédagogique » à l'égard des autorités ? Une telle fonction de sensibilisation aux produits du renseignement pourrait davantage aider à éviter, dans la phase de communication, les deux pièges que sont d'une part, le désintérêt et la non-utilisation du renseignement par l'autorité et d'autre part, l'éventuel usage du renseignement pour une fin non conforme à sa finalité (comme par exemple un objectif purement médiatique).

Des exemples étrangers montrent l'intérêt pour les services d'expliquer de manière constante leurs missions. Bien évidemment, ces dernières sont circonscrites dans un cadre bien défini par les autorités politiques, mais cet encadrement ne peut aller jusqu'à influencer l'objectivité des analyses des services concernés.

En ce qui concerne la Belgique, le Comité permanent R a plutôt le sentiment que le potentiel des renseignements produits par les services n'est pas suffisamment préparé et spécifiquement accompagné pour que les autorités puissent les utiliser d'une manière optimale.

Pour illustrer plus avant son propos général, le Comité permanent R constate encore à ce jour que dans certains domaines comme l'islamisme radical, les analyses des deux services ne sont pas toujours concordantes, ce qui résulte sans doute dans ce domaine d'une collaboration sujette à caution et peut-être aussi parfois d'options stratégiques différentes dans une matière touchant à la sphère internationale (et donc aussi à la coopération avec les services de renseignement et de sécurité d'autres états européens et tiers).

Le Comité permanent R tient enfin à rappeler que dans la sphère du renseignement, il distingue l'apport indispensable d'informations par la Sûreté de l'Etat et le SGRS dans la cadre d'enquêtes judiciaires, du traitement et de l'analyse de ces informations dans le contexte des menaces à rapporter aux autorités administratives, telles qu'elles sont définies par la loi organique des services de renseignement et de sécurité du 30 novembre 1998.

C'est essentiellement, à ce niveau, que se situe pour le Comité permanent R, une des différences essentielles entre l'action des services de police et de renseignement, ainsi que la spécificité des missions de ces derniers.

Dans son rapport général d'activités 2000, se référant à la collaboration accrue demandée par le Conseil Justice et Affaires intérieures de l'Union européenne le 20 septembre 2001, le Comité permanent R écrivait qu'il était d'avis que « *la collaboration entre les services de renseignement doit viser l'analyse des menaces à long terme, tandis que la collaboration de ces services avec les services de police doit porter sur les menaces à court terme et la recherche des auteurs d'actes terroristes ».*

Si les définitions sont claires, la pratique est sans doute toute autre et souvent plus floue. Si elle génère incontestablement des résultats positifs, elle est susceptible aussi, sans véritable coordination et sans contrôle constant, de générer des dysfonctionnements graves.

5. LA COLLABORATION INTERNATIONALE AVEC LES SERVICES ÉTRANGERS

Cette matière constitue également un des centres d'intérêts du Comité permanent R. Celui-ci a pu constater, toutefois, au cours des années qu'il s'agit d'un domaine où les services de renseignement sont peu enclins à la transparence.

Dans ses rapports d'activités précédents, le Comité permanent R a maintes fois évoqué cette problématique *(voir e.a. « La manière dont les services de renseignements ont traité les activités de l'ancien KGB en Belgique » rapport général d'activités 2000 - p. 78-90 ; « Rapport de l'enquête sur la manière dont la SE s'acquitte de sa nouvelle mission de protection du potentiel scientifique et économique » et plus particulièrement « Le rôle des Services de renseignements en matière économique à l'étranger » rapport général d'activités 2000- p. 112-147 ; « L'enquête de contrôle concernant le fonctionnement des services de renseignement belges dans la gestion d'éventuelles informations dans un contexte préalable à la passation d'un marché international » rapport général d'activités 2001 - p. 5-7 ; « Rapport sur la participation de la Sûreté de l'Etat aux réunions ILETS » rapport général d'activités 2001- p. 17-22 ; « Brève évaluation de l'efficacité des Services de Renseignement au 8 octobre 2001 » et plus particulièrement le point « La collaboration internationale avec des services étrangers » rapport général d'activités 2001- p. 183-194) »*

Il faut rappeler que la coopération entre les services de renseignement sur le plan international est dominée par des règles spécifiques. En premier lieu, il faut citer la règle du tiers selon laquelle « le service qui reçoit une information d'un service étranger n'est pas autorisé à la diffuser en dehors des services de police et de renseignement nationaux concernés, sauf accord exprès de l'Etat qui a fourni l'information, celui-ci se réservant en outre le droit d'apprécier le besoin d'en connaître du destinataire éventuel (' need to know')» (rapport général d'activités 2001 - p. 199 citant le document (EUROPOL - INFOPOL 69 du 13 juillet 2001).

Un second principe est celui-ci du « donnant-donnant». Pour recevoir une information d'un service étranger, il faut être en mesure de lui en fournir un autre de même valeur en échange.

En troisième lieu, il convient d'évoquer les règles de classification qui limitent aussi à leur manière l'utilisation des informations transmises, notamment dans le fait que seule celle des parties qui a déterminé le degré de classification peut le modifier.

Celui qui est seulement familier des opérations judiciaires sur le plan national peut se poser des questions au sujet de l'efficacité de tels principes de travail.

Il ne faut toutefois pas perdre de vue le fait que chaque Etat a droit au respect de sa souveraineté et que les intérêts de chaque Etat - dont les services de renseignements doivent assurer la protection contre diverses menaces - peuvent être différents et même opposés. Il suffit de se référer à la nécessité de la protection du potentiel économique et scientifique d'un pays, pour comprendre que même des services « alliés » ne peuvent pas l'être pour toutes les missions. Les points de vue divergents entre Etats sur des problèmes de politique internationale constituent un autre exemple.

Enfin, pour des raisons qui tiennent aux principes spécifiques de fonctionnement, l'échange d'informations entre les services de renseignement se réalise selon des canaux propres, distincts des circuits de coopération internationaux policiers et judiciaires.

Les formes actuelles de la criminalité organisée et principalement les actions particulièrement violentes du terrorisme international appellent à s'interroger sur le renforcement et l'instauration d'autres formes d'échange d'informations, ainsi que sur le contrôle de celui-ci tant au niveau national qu'au niveau européen.

Sans doute aussi faut-il s'interroger sur la subsistance au sein du monde du renseignement d'une culture héritée de la guerre froide où pour les deux sphères d'influence, l'ennemi était bien identifié, connu et localisé. C'est l'évidence aujourd'hui que les menaces sont multiformes, délocalisées et particulièrement fluides.

En ce qui concerne la collaboration internationale, le Comité permanent R a dressé durant la période d'activités 2003 « un rapport intermédiaire relatif à l'enquête sur la manière dont la Sûreté de l'Etat répond aux demandes des services de renseignement étrangers ayant un représentant dans le royaume »

Ce rapport qui est repris en page 217 souligne des difficultés certaines dont la moindre n'est sans doute pas celle qui résulte en la matière d'une culture extrême et sans nuance du secret.

Le Comité permanent R estime que la Règle du Tiers appliquée sans aucun contrôle ne peut constituer un automatisme qui aurait comme implication de déplacer de manière quasi exclusive et peut-être même parfois dangereuse, le pouvoir politique d'un Etat vers un service de cet Etat.

Le Comité permanent R a déjà signalé que l'interprétation stricte de cette règle coutumière à son égard notamment, dresse un obstacle à un contrôle efficace.

Dans son rapport général d'activité 2001, le Comité permanent R mentionnait en ce qui concerne la coopération européenne des services de renseignement en matière de lutte contre le terrorisme « qu'à l'instar des conclusions de la Conférence PARLOPOL tenue à Bruxelles, les 15 et 16 octobre 2001, cette collaboration internationale devrait aussi faire l'objet d'un contrôle parlementaire »

Enfin, le Comité permanent R s'est enquis en 2003 de l'état des relations que le SGRS et la Sûreté de l'Etat entretenaient avec leurs correspondants américains et britanniques alors que la Belgique n'était pas associée à la coalition militaire contre le régime de Bagdad.

Les réponses respectives des deux services concordent sur le fait qu'indépendamment des prises de positions politiques, l'état des relations avec les services de ces deux pays n'en avait été nullement affecté dans leurs domaines d'intérêt. Au contraire, toujours aux dires des services belges, on a pu assister à une augmentation qualitative et quantitative des échanges.

Il n'en reste pas moins que cette collaboration demeure une matière hautement sensible et difficile à circonscrire.

Depuis hélas, les attentats dramatiques des 11 septembre 2001 et 11 mars 2004, le Comité permanent R suit avec un intérêt accru les discussions concernant la coopération internationale des services de renseignement.

6. LA COOPÉRATION ENTRE LA SURETE DE L'ETAT ET LE SGRS

Dans son rapport général d'activités 1999, le Comité permanent R publiait un 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. »

La collaboration y était décrite comme fructueuse par l'un et l'autre des services. Le Comité permanent R avait regretté toutefois que des comptes rendus des réunions communes ne soient pas systématiquement rédigés. Pour le Comité permanent R, il s'agissait là, non seulement d'un manque de rigueur, mais également d'une atteinte à la possibilité d'un contrôle a posteriori efficient.

Dans le rapport général d'activités 2001 du Comité permanent R, il était mentionné, toujours concernant le même protocole, que son application était qualifiée de satisfaisante par les responsables des deux services.

Le Comité permanent R constatait toutefois que des enquêtes de contrôle faisaient apparaître des signes ponctuels d'un déficit de collaboration entre le SGR et la Sûreté de l'Etat, notamment dans le cadre des nouvelles missions attribuées à ce service par la loi organique déjà citée de 1998.

Le Comité permanent R déduisait de ces constatations que « la collaboration systématique entre ces services n'est pas encore bien encrée dans leurs mentalités respectives et que des méfiances réciproques subsistent » (rapport général d'activités 2001 - p191).

En 2002, le Comité permanent R constatait de plus que « le protocole d'accord entre la Sûreté de l'Etat et le SGRS n'était plus d'application dans la matière de l'islamisme extrémiste ». Pour le surplus, le Comité permanent R avait aussi pointé du doigt à plusieurs reprises que « la Sûreté de l'Etat considérait que le suivi général de la menace lié à l'extrémisme islamiste ne relevait pas de la compétence légale du SGRS ».

Le rôle et la responsabilité de l'organe de contrôle, particulièrement dans le contexte actuel, sont de signaler que depuis les attentats du 11 septembre 2001, des tensions sont en effet perceptibles entre la Sûreté de l'Etat et le SGRS au sujet du suivi de la menace des activités extrémistes et terroristes islamistes.

Le point de départ de ces tensions semble se situer, selon l'analyse du Comité permanent R, au moment où, après les attentats de New York, le SGRS a adapté ses plans directeurs du renseignement et de la sécurité pour les mettre en adéquation avec l'actualité. Jusqu'au 11 septembre, en effet, l'extrémisme et le terrorisme islamistes ne constituaient pas une priorité du SGRS.

Pour rappel, l'extrémisme et le terrorisme islamique sont traités par deux sections du SGRS dans la mesure où ces menaces concernent la sécurité des forces armées en Belgique et à l'étranger (principalement dans les Balkans). Il s'avère aussi que les intérêts militaires situés en Belgique (le siège de l'OTAN par exemple) sont aussi susceptibles d'être pris pour cibles d'actions terroristes.

Les missions du Service général de renseignement et de sécurité, définies par l'article 11 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité s'inscrivent, en effet, dans le contexte de la défense des intérêts militaires.

La Sûreté de l'Etat a, quant à elle, en vertu des articles 7 et 8 de la même loi une compétence générale en matière de menaces en relation avec le terrorisme et l'extrémisme.

Lors des discussions de la loi en projet, le gouvernement avait souligné que « *des chevauchements partiels découlent de la définition des missions de la Sûreté de l'Etat et de celle du SGR. Ces services sont, par exemple, tous deux compétents pour veiller à la sauvegarde de l'intégrité du territoire national* » (Doc. parl. Sénat – session 1997-1998 – n° 758/10 – rapport fait au nom des commissions réunies de la Justice et des Affaires étrangères – p. 14).

Des discussions théoriques concernant ces problèmes de compétence sont toujours en cours, depuis un certain temps, entre les deux services dans le cadre de la révision et de l'adaptation du protocole d'accord – qui les lie depuis 1997 – aux dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Dans le cadre de la collaboration bilatérale entre les deux services, la Sûreté de l'Etat a fait part au Comité permanent R de son souci d'éviter d'une manière générale qu'un double travail soit effectué. La Sûreté de l'Etat estime que les ressources des services sont trop limitées que pour accepter une dispersion des forces que la loi précitée a souhaité éviter.

Si effectivement la juste limite des compétences de chaque service n'est pas toujours facile à établir, et que le Comité permanent R peut d'autre part partager le point de vue de principe de la Sûreté de l'Etat, il estime néanmoins qu'aucune définition théorique ne pourra régler le problème sans que sur le terrain et dans un climat de confiance, la coopération et la concertation des différents acteurs ne soient effectivement assurée de manière coordonnée.

Le Comité permanent R attire aussi l'attention sur le fait qu'il ne faudrait pas que des divergences dans l'interprétation des dispositions légales réglant les compétences de chacun des services constituent un prétexte ou un alibi pour justifier l'instauration d'un climat de méfiance et un repli dans la coopération effective des deux services de renseignement.

Dans le domaine de l'extrémisme islamiste et dans le cadre d'enquêtes de contrôle en cours, le Comité permanent R ne peut que rendre compte une nouvelle fois, du constat selon lequel les perceptions stratégiques de la menace se situent souvent à des niveaux différents de gravité selon l'un ou l'autre des services. Cela donne à penser au Comité permanent R que de réels efforts doivent être entrepris pour rencontrer sur le terrain l'obligation légale faite aux services de renseignement (article 20 de la loi organique précitée du 30 novembre 1998) « d'assurer une collaboration aussi efficace que possible ».

Cette constatation renforce la conviction du Comité permanent R, qu'au-delà de la discussion et de la conclusion de protocoles et d'accords formels, existe une impérieuse nécessité d'une coordination réelle du renseignement à un niveau supérieur de l'Etat.

7. LA PROTECTION DES DROITS INDIVIDUELS DE LA PERSONNE

La question peut être légitimement posée de savoir si l'attribution à un organe de contrôle de deux missions contradictoires en apparence comme d'une part l'efficacité des services de renseignement et, d'autre part la protection des droits et libertés des citoyens, permet de rencontrer en même temps ces deux objectifs avec la même efficience.

Le Comité permanent R a pu expérimenter que la prise en considération permanente des deux approches dans la problématique d'un contrôle externe, est certes un exercice difficile, mais indispensable et même incontournable tant les deux aspects sont malgré leur apparente opposition, intimement liés.

C'est ainsi qu'en se référant au rapport de l'enquête « sur la manière dont les services de renseignement s'intéressent aux activités islamistes extrémistes et terroristes » (rapport général d'activités 2001 - p. 81 et suivantes), le Comité permanent R rappelle que lors du début de cette enquête de contrôle en 1998, un de ses premiers objectifs était de vérifier si dans le suivi de cette problématique, et dans le contexte de l'élection des membres de « l'organe chef du culte musulman », les services respectaient les libertés et droits individuels des adeptes du culte islamique.

Au cours de l'enquête, le problème de la communication insuffisante aux autorités politiques du danger de la menace extrémiste par les services de renseignement, s'est imposé comme un élément important. Cette constatation a justifié la nécessité de s'intéresser également à l'efficacité de l'évaluation de la menace elle-même.

Le rapport de « l'enquête de contrôle et la plainte concernant madame Soetkin Collier » (voir ci-après p. 134) illustre l'approche diamétralement opposée puisqu'en l'espèce, le contrôle sur la manière de fonctionner du service de renseignement a suscité la question de la protection des droits individuels à l'occasion de la communication de renseignements à l'autorité.

Les constatations effectuées, aussi bien dans l'une et l'autre de ces enquêtes sur l'utilisation d'informations recueillies par les services de renseignement, à d'autres fins et dans le cadre d'autres procédures, ont entraîné une réflexion de principe plus large du Comité permanent R.

Le Comité permanent R a principalement relevé que dans treize domaines identifiés, la Sûreté de l'Etat délivrait, sans véritables bases légales, des informations de nature individuelle ou des avis à d'autres autorités. Le même problème se pose également pour le SGRS, mais dans une moindre mesure puisque ce service est moins sollicité pour fournir des avis dans des procédures administratives. Cela n'empêche pas que le raisonnement sur le plan des principes et du droit sont également applicables à ce service.

Le Comité permanent R avait déjà constaté dans le cadre de plaintes de particuliers (voir ci-après Titre II – Point d) que de telles procédures étaient susceptibles d'entraîner des conséquences préjudiciables aux personnes concernées qui pour le surplus ne disposaient pas de moyens suffisants pour obtenir une réparation du dommage éventuel.

De manière contemporaine, Madame la Ministre de la Justice a demandé *« l'avis du Comité permanent R concernant le cadre juridique dans lequel la Sûreté de l'Etat et le SGRS peuvent procéder à des vérifications de sécurité sur des personnes et transmettre des avis et informations à caractère personnel aux autorités. »*

Cet avis est reproduit en page 263 du présent rapport général d'activités 2003.

Le Comité permanent R estime ainsi, à l'instar du législateur, qu'il est légitime que partant de son contrôle de l'efficacité des services, il s'attache à mettre en évidence les conséquences que le renforcement de cette efficacité peut générer sur le plan des libertés et des droits fondamentaux des personnes.

8. PRIORITES DU COMITE PERMANENT R

En conclusion de cette introduction générale et sur la base des éléments qui y sont contenus, le Comité R voudrait mettre l'accent sur les trois priorités suivantes :

8.1. Le cycle du renseignement

Outre les problèmes liés à la problématique générale du flux de l'information que le Comité permanent R aborde dans le contexte d'enquêtes de contrôle thématiques, l'évolution de la coopération et de la coordination du renseignement entre la Sûreté de l'Etat et le SGRS, continuera à retenir l'attention particulière de l'organe de contrôle.

Cette attention portera non seulement sur l'exécution dans la pratique des compétences respectives des deux services, mais également sur l'aspect formel de l'élaboration entre ces derniers d'un nouveau protocole d'accord.

L'enquête commune des Comités P et R, déjà évoquée ci-avant, devra compléter la vision que l'on peut avoir de la coordination entre les services de sécurité dans la lutte contre le terrorisme en incluant dans l'analyse les relations entre le renseignement et les services de police.

Le renseignement implique en effet d'autres autorités et d'autres acteurs qui dépassent le champ de compétence du Comité permanent R. Celui-ci n'est qu'un rouage dans le système de contrôle mis en place par la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

C'est la raison pour laquelle le Comité permanent R estime prioritaire que le suivi de ces activités puissent également continuer à se développer au niveau des échanges de vues avec les commissions ad hoc du Sénat et de la Chambre ainsi qu'avec les ministres compétents.

Le Comité permanent R estime également que des contacts plus suivis avec d'autres institutions dont certaines dépendent également du Parlement, comme par exemple, la Commission pour la Protection de la Vie Privée, le Centre pour l'Egalité des Chances, les Médiateurs Fédéraux pourraient, sous certains aspects, apporter des compléments d'information ou d'expérience réciproques utiles aux missions respectives de chacune de ces institutions.

8.2. Le Contrôle des interceptions de communications émises à l'étranger par le SGRS

Le Comité permanent R attache comme il se doit une importance toute particulière à cette nouvelle compétence qui devra au cours de l'année 2004 prendre tout son essor, après une phase de préparation qui a eu lieu dans les derniers mois de 2003.

En plus de son aspect particulier, le Comité permanent R estime que d'une manière semblable à sa compétence d'organe de recours en matière d'habilitations de sécurité, cette nouvelle compétence contribuera à affiner sa connaissance des spécificités et des problèmes relatifs à la matière du renseignement.
Cette approche permettra éventuellement au Comité permanent R de rencontrer dans l'avenir d'autres compétences similaires dans le domaine des interceptions de sécurité.

8.3. La protection des libertés et droits individuels

Que ce soit dans le cadre de ses activités de contrôle, à la suite de plaintes de particuliers ou dans l'exercice de ces autres compétences, le Comité permanent R met plus que jamais une priorité à se consacrer à cet aspect de sa mission.

En complément aux réflexions qui sont les siennes en cette matière et qui sont publiées ci-après (p. 263) le Comité permanent R inclut également dans ses priorités la recherche d'une meilleure information du plaignant quant aux suites des enquêtes de contrôle. Vu le caractère à la fois délicat et incontournable du problème, le Comité permanent R en a déjà saisi, par ailleurs, sa Commission de suivi dans le but de trouver une solution équilibrée.

TITRE II : LES ENQUETES DE CONTROLE

A. *ENQUETES A LA REQUETE DU PARLEMENT* OU DES MINISTRES

CHAPITRE 1: LA PROTECTION DU POTENTIEL SCIENTIFIQUE OU ÉCONOMIQUE DU PAYS : LE RÔLE DES SERVICES DE RENSEIGNEMENT PRIVÉS ET PUBLICS.

"Aujourd'hui, les conflits ne sont plus systématiquement ouverts ni déclarés. Les agressions économiques notamment sont plus sournoises, elles peuvent déstabiliser gravement nos sociétés modernes. Le XXIème siècle, qui sera celui de la complexité, nécessite dès aujourd'hui la conception et la mise en oeuvre d'une stratégie globale répondant au défi. La cohérence et l'efficacité de cette démarche ne seront garanties que si la société civile et l'Etat maintiennent des échanges permanents et translatéraux".

Marc LADREIT de LACHARRIERE, Président de l'Institut d'études et de recherches pour la sécurité des entreprises (Paris)

INTRODUCTION

La loi du 30 novembre 1998 organique des services de renseignement et de sécurité ([7]) a confié une nouvelle mission à la Sûreté de l'Etat, à savoir la recherche, l'analyse et le traitement du renseignement « *relatif à toute activité qui menace ou pourrait menacer (…) le potentiel scientifique ou économique* » du pays tel que défini par le Comité ministériel du renseignement. A l'occasion des travaux préparatoires de cette loi de 1998, le Comité permanent R avait préconisé la création d'un organe de concertation entre les entreprises détentrices d'un potentiel scientifique ou économique vital pour la Belgique et les ministres concernés par cette matière. Il avait également indiqué qu'il ne faudrait pas négliger de fournir à la Sûreté de l'Etat les moyens qu'elle réclamait au risque de voir l'exécution de cette nouvelle mission rester lettre morte.

Depuis l'année 1998, à travers les différentes enquêtes qu'il a menées, le Comité permanent R s'est régulièrement intéressé à la manière dont la Sûreté de l'Etat avait pris en charge sa nouvelle mission de protection du potentiel scientifique ou économique. C'est dans ce cadre que le Comité a notamment attiré l'attention sur l'émergence des sociétés privées qui se spécialisent dans le renseignement ou l'intelligence économique au profit d'entreprises ou d'autorités publiques, d'où la question d'un contrôle sur ce type d'activités.

Le 13 novembre 2003, au cours du colloque organisé à Bruxelles pour célébrer les dix années d'existence de la loi sur la fonction de police, M. Herman De Croo, président de la Chambre des représentants a rappelé cette conclusion du plan fédéral de sécurité : *« afin de soumettre les acteurs privés de la sécurité à un contrôle démocratique, il convient de voir si les Comités permanents de contrôle des services de police et de renseignements peuvent apporter leur contribution en la matière dans les limites de leur mission légale ».* Le présent rapport constitue la première contribution que le Comité permanent R tente d'apporter dans cette matière.

[7] Moniteur belge du 18 décembre 1998.

Le présent rapport, complété et actualisé au 31 décembre 2003, porte sur les études et les enquêtes que le Comité permanent R a menées sur la protection du potentiel scientifique et économique ainsi que sur le rôle des services de renseignement privés depuis l'année 1998([8]).

AVERTISSEMENT

Le présent rapport aura plusieurs fois recours aux notions de « renseignement économique », « d'Intelligence économique », d' « espionnage économique », d' « espionnage industriel », d' « espionnage de concurrence » ou encore de « service de renseignement privé ». Ces concepts font l'objet de nombreuses définitions plus ou moins semblables ou divergentes selon les écoles. Tout au long de la rédaction du présent rapport, le Comité permanent R s'est donc heurté à la difficulté de ne pas pouvoir se référer à des définitions unanimement reconnues de ces notions pourtant largement utilisées. Devant ce flou terminologique qui caractérise cette problématique, le Comité permanent R s'est résolu de ne s'attacher à aucune des nombreuses définitions proposées par la littérature consacrée au sujet. Le présent rapport vise plutôt à décrire de manière générale la problématique de la protection du potentiel scientifique et économique par un service de renseignement étatique confronté ou en concurrence avec une palette d'activités de recherches d'informations et de services dits de sécurité que certaines firmes privées ou services d'Etats développent dans les milieux économiques.

Certaines propositions de définitions apparaîtront cependant au cours du présent rapport. Il s'agira de quelques notions de base à propos desquelles la littérature spécialisée et les auteurs semblent s'entendre.

En décidant de reconnaître ce vaste domaine de la protection du potentiel scientifique et économique, le Comité permanent R a pris le risque délibéré de s'aventurer dans des domaines extérieurs mais connexes au monde du renseignement.

REMERCIEMENTS

Le Comité permanent R remercie les personnes suivantes qui ont contribué à la rédaction du présent rapport.

- Messieurs Claude Moniquet et Frédéric Moser, experts du Centre européen pour le Renseignement stratégique et la Sécurité ;
- Monsieur Wauter Van Laethem, juriste et Madame Aline Goosens, documentaliste, collaborateurs du Comité permanent R.

PLAN DE L'ETUDE

Tenter de décrire la mission de protection du potentiel scientifique et économique de la Sûreté de l'Etat nécessite que soient posées les questions fondamentales suivantes :

[8] Ces questions ayant fait l'objet de nombreuses études ainsi que d'un débat parlementaire en France, le lecteur ne sera pas étonné de trouver de nombreuses références françaises dans la présente étude.

1. Qu'est-ce que le potentiel scientifique ou économique d'un pays, et singulièrement, celui de la Belgique ?

2. Qui sont les moteurs du développement du potentiel scientifique et économique d'un pays comme le nôtre ?

3. A quelles menaces est exposé notre potentiel scientifique et économique ? Dans cette partie du rapport, on examinera particulièrement l'essor des activités des firmes privées de renseignement qui peut être considéré soit comme une opportunité de développement, soit comme une nouvelle menace pour le monde scientifique et économique.

4. A quelles difficultés se heurte la protection de notre potentiel scientifique et économique ?

5. Quelles missions et quels moyens d'action les gouvernements peuvent-ils donner aux services de renseignement pour protéger le potentiel scientifique et économique de leur pays ? Fidèle à sa méthode d'analyse comparative, le Comité permanent R examinera ici le rôle de certains services étrangers, publics et privés, en matière de recherche de renseignements et de protection du potentiel scientifique et économique.

6. Quel est l'état du marché du renseignement privé en Belgique ?

7. Quels moyens l'arsenal législatif belge permet-il de mettre en œuvre afin de protéger les secrets intéressant le potentiel scientifique et économique du pays ?

8. Quelles sont les attentes des milieux économiques belges à l'égard de la Sûreté de l'Etat ?

9. Que font les services de renseignement belges ? Quelle est leur attitude à l'égard des services de renseignement privés ?

10. Bien que ces questions concernent essentiellement la Sûreté de l'Etat, le Comité permanent R pense qu'il convient aussi d'associer le Service Général du Renseignement et de la Sécurité (SGRS) des Forces armées à la réflexion.

Après quoi seront tirées des conclusions (10) et des recommandations (11).

1. COMMENT DÉFINIR LE POTENTIEL SCIENTIFIQUE OU ÉCONOMIQUE D'UN PAYS COMME LE NÔTRE ?

Le premier rapport que le Comité permanent R a consacré à cette matière faisait déjà apparaître la difficulté de cerner la notion de potentiel scientifique ou économique. Au sens des articles 7, 1° et 8, 4° de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, on entend par "*potentiel scientifique ou économique*" , "*la sauvegarde des éléments essentiels du potentiel scientifique ou économique*". Il appartient au Comité ministériel du Renseignement et de la Sécurité de définir plus avant cette notion.

En juillet 2000, le Conseil des ministres a pris connaissance d'une note d'orientation du ministre de l'Economie et de la Recherche scientifique relative à l'évolution de la politique scientifique fédérale. Le Comité permanent R a cherché dans ce document quelques éléments susceptibles de préciser davantage la notion de potentiel scientifique ou économique.

Cette note indique que l'économie est plus que jamais fondée sur la connaissance; elle souligne qu'environ 50% de la croissance économique est liée aux nouvelles technologies et aux nouveaux produits. La recherche scientifique est donc devenue une préoccupation majeure tant au niveau européen que national. En Belgique, la politique scientifique ressort des Services fédéraux des Affaires scientifiques, techniques et culturelles (SSTC en abrégé). La note d'orientation ne donne guère d'indications sur les recherches scientifiques de pointe effectuées en Belgique; elle souligne cependant la qualité des recherches et des technologies en Belgique.et, notamment de leur applications spatiales

Le ministre de l'Economie et de la Recherche scientifique annonce seulement son intention de procéder à une évaluation du potentiel scientifique présent dans les "pôles d'attraction technologiques" (PAT) et "Pôles d'attractions Inter universitaires" (PAI) en Belgique. Il annonce aussi son intention "*de mettre à la disposition des centres de recherches fédéraux et des Interfaces universités-entreprises des universités belges, des agents chargés de la prospection dans les secteurs de pointe afin de renforcer notre capacité de transferts technologiques*"

Il faut noter pour le surplus que la mise en œuvre de la politique économique du pays est de la compétence des trois régions fédérées.

La notion corollaire de **sécurité économique**, objectif général auquel doivent en principe tendre tous les gouvernements, a été définie comme suit par le Service canadien du renseignement de sécurité : *"L'époque où la question de la sécurité mondiale primait sur les préoccupations d'ordre économique et les conflits régionaux dans les relations internationales est révolue. L'interdépendance économique et la concurrence internationale croissantes sont devenues des sources importantes de tensions et de conflits entre les puissances mondiales. Dans ce climat d'incertitude, les pays industrialisés qui désirent vivement maintenir leur niveau de vie et les pays en développement qui sont tout aussi déterminés à améliorer le leur sont poussés à utiliser tous les moyens à leur disposition pour améliorer leur productivité et assurer leur sécurité économique. L'un de ces moyens est l'espionnage économique (...)"* ([9]).

En France, la sécurité économique consiste à veiller à ce que les moyens, connaissances ou informations permettant de préserver les intérêts essentiels de la nation, soient conservés sous le contrôle français et qu'ils soient développés et adaptés en permanence à l'évolution du contexte et des risques géostratégiques mondiaux ([10]).

---

9 "*La sécurité économique*", rapport du Service canadien du renseignement de sécurité paru dans *"Série d'aperçus"* n° 6, mai 1998 - www.csis-scrs.gc.ca

10 *"De la défense économique à la sécurité de l'économie"*, Jean-Louis Levet - rapport du Commissariat général du Plan, 1997

Au Canada, on entend par sécurité économique le fait de maintenir des conditions propres à favoriser une augmentation relative soutenue et à long terme de la productivité du travail et du capital, ce qui assure à la population un niveau de vie élevé et en progression constante, et garantit un environnement économique équitable, sûr et dynamique, propice aux innovations, aux investissements intérieurs et étrangers, ainsi qu'une croissance soutenue ([11]).

On verra plus loin dans la présente étude ([12]), qu'au cours de l'année 2001, la Sûreté de l'Etat a adressé au Comité ministériel du renseignement et de la sécurité une note contenant une série de propositions relatives à la définition du potentiel scientifique et économique, à l'établissement de priorités, à la détermination des menaces qui visent ce potentiel, ainsi qu'une description des missions qui devaient incomber à la Sûreté de l'Etat en cette matière.

Ces propositions n'ont cependant pas été approuvées par le Comité ministériel du renseignement de la Sécurité, ce qui illustre la difficulté de définir le potentiel scientifique et économique d'un pays comme la Belgique.

2. QUI SONT LES MOTEURS DU POTENTIEL SCIENTIFIQUE ET ÉCONOMIQUE D'UN PAYS COMME LA BELGIQUE ?

A cet égard, la situation se caractérise par la diversification et l'hétérogénéité croissante des acteurs du potentiel scientifique et économique d'un pays. A côté de l'Etat lui-même, de ses infrastructures, de ses services, entreprises publiques autonomes (SNCB, Belgacom, etc.), on trouve les entités fédérées (communautés et régions), les universités, hautes écoles et autres organismes d'intérêt public, les entreprises privées novatrices et à forte valeur ajoutée, les laboratoires de recherches, ainsi que leurs personnels qui, chacun avec une logique propre, les uns de service public, les autres de profit, occupent une place majeure, non seulement dans l'économie marchande, mais aussi dans la recherche scientifique, technologique, les services collectifs, la culture et les relations internationales.

Ceci implique qu'une liste de secteurs d'activités vitales à protéger dans ces différents secteurs soit établie en définissant un ordre de priorité. Il faut toutefois être conscient que les restructurations industrielles et la globalisation des procédés au niveau mondial rendent difficile l'attribution d'une nationalité aux entreprises.

Les responsables politiques, dirigeants, fonctionnaires, entrepreneurs, cadres, actionnaires chercheurs et autres membres du personnel participant au développement du potentiel scientifique ou économique, doivent être conscients des activités qui peuvent menacer leur secteur et du rôle qu'ils peuvent jouer pour le protéger.

Préférant la définition de secteurs et de domaines prioritaires à l'énumération nominative de structures et d'organisations économiques et scientifiques, la Sûreté de l'Etat propose de considérer comme prioritaires les domaines d'activité suivants :

- les entreprises publiques autonomes (loi du 21 mars 1991),
- les organismes d'intérêt public (loi du 21 mars 1991),
- les entreprises vitales pour les besoins de la population (eau, gaz, électricité, carburant, transport, etc.),

---

11 "Série d'aperçus" n° 6 - mai 1998, publication du Service Canadien de Renseignement de Sécurité.

12 Voir plus loin le point 8.1.4.

- les entreprises, centres de recherche, universités, hautes écoles, services publics et les autres structures créées sur le plan supranational, international, fédéral et régional dont les activités ont trait à des secteurs technologiques de pointe, notamment la technologie spatiale, l'aéronautique, la santé, l'énergie, l'informatique, les télécommunications, l'environnement, la biotechnologie, la chimie et le secteur nucléaire.

3. A QUELLES MENACES EST EXPOSÉ LE POTENTIEL SCIENTIFIQUE ET ÉCONOMIQUE DE NOTRE PAYS ?

Dans une note interne, la Sûreté de l'Etat identifie les menaces suivantes :

- les activités émanant de groupements idéologiques, sectaires, terroristes ou criminels,
- les attentats ou sabotages visant la destruction physique d'infrastructures,
- la déstabilisation de l'économie par la corruption, le blanchiment et l'introduction de capitaux provenant d'activités criminelles,
- les activités clandestines de puissances étrangères (l'espionnage économique) ou d'entreprises étrangères (l'espionnage de concurrence) qui peuvent nuire aux intérêts belges dans le domaine scientifique et économique,
- les activités commerciales de recueil, de traitement et d'analyse d'informations qui peuvent porter atteinte au potentiel scientifique et économique,
- la fabrication et la diffusion d'informations comme moyen de désorganisation dans les secteurs d'activité d'intérêt essentiel pour le bon fonctionnement des institutions fédérales et régionales, les universités, les écoles supérieures, les institutions de recherche et les entreprises : ceci vise les campagnes organisées de désinformation et d'influence (le lobbying) dans le but de porter atteinte au potentiel scientifique et économique.

En France, un rapport parlementaire intitulé « *Intelligence économique, compétitivité et cohésion sociale* » ([13]) décrit les nouvelles menaces qui pèsent sur les entreprises françaises :

- la grande perméabilité des services financiers aux comportements criminels et mafieux ;
- le détournement et la captation d'informations notamment dans les marchés de la sécurité et du renseignement privés ;
- l'utilisation de la désinformation comme procédé de concurrence déloyale ;
- les dépendances stratégiques d'entreprises (d'approvisionnement, technologiques,) à l'égard de fournisseurs étrangers ;
- les puissantes organisations criminelles transnationales.

Au cours d'un séminaire organisé en septembre 2003 par l'Institut CERAM de Sophia Antipolis (Nice) sur le thème « *Intelligence économique et Management des Risques* », des représentants d'industries et de milieux économiques français ont cité les principaux risques auxquels ils estimaient être exposés.

Aux côtés des menaces classiques de la concurrence (américaine, britannique et russe) et de l'espionnage, certains intervenants citent aussi les organisations criminelles dont le degré de dangerosité n'est pas assez reconnu, ainsi que le terrorisme et l'islamisme radical. Sont aussi citées… des Organisations Non Gouvernementales (ONG) auxquelles on reproche de nuire aux intérêts économiques sous prétexte de défendre des valeurs comme les droits de l'Homme, l'éthique, l'écologie et l'environnement.

---

[13] Rapport au Premier ministre du député Bernard Carayon, juin 2003, voir plus loin le point 5.2.3.

Une étude menée en Grande Bretagne par le cabinet *Risk Advisory Group* en 2002 indique en effet que, bien avant le terrorisme ou la criminalité financière, les dirigeants d'entreprises craignent d'abord les attaques contre leur réputation, leurs marques ou leur enseigne.

Le présent rapport s'intéressera tout particulièrement aux activités de recueil, de traitement et d'analyse d'informations qui se développent dans le secteur privé et le monde économique. Ces activités offrent sans conteste de nouvelles opportunités de développement économique mais elles sont aussi susceptibles de porter atteinte au potentiel scientifique et économique d'un pays lorsque, dépassant le cadre de la veille ou de l'intelligence économique[14], elles visent à s'approprier des secrets scientifiques et / ou économiques au moyen de pratiques proches de l'espionnage. Ces pratiques seront définies et examinées plus loin dans le présent rapport.

3.1. Le développement du renseignement privé : menace ou opportunité pour le potentiel scientifique et économique ?

Comme on le verra dans les chapitres suivants, la collecte d'informations par des firmes privées peut avoir pour objectif :

- de maintenir ou d'accroître le potentiel économique d'entreprises dans un cadre concurrentiel d'une part (on parlera alors de *renseignement économique* ou d'*intelligence économique*),

- d'assurer la sécurité physique de leur personnel, de leur patrimoine et de leurs installations d'autre part (on parlera alors de *renseignement de sécurité).*

De nos jours, la diffusion croissante de l'information a ceci de particulier qu'elle a eu pour conséquence de lui conférer une valeur marchande grandissante. L'information en elle-même n'a qu'une valeur limitée, c'est son traitement qui lui confère son statut et la transforme en renseignement. Cela signifie que devant la multiplication des sources dites ouvertes et devant leur plus grande accessibilité, le temps d'accès est devenu un facteur qui détermine le temps de réaction de l'entreprise. C'est ce qui explique notamment la multiplication des cabinets de consultants spécialisés dans la recherche de l'information qui fournissent à l'entreprise son information stratégique au moment pertinent, c'est-à-dire avant la concurrence, et pour lui permettre de guider son processus décisionnel.

En effet, les lois ordinaires du marché ne permettent plus à elles seules d'expliquer les succès ou les échecs des entreprises. L'économie de l'immatériel s'est considérablement développée, notamment via internet. Les échanges d'informations se sont considérablement accrus tant en densité qu'en rapidité. L'Intelligence économique cherche à gérer l'ensemble des flux d'informations liés au renseignement susceptible d'intéresser l'entreprise. Elle permet la formulation de certains choix stratégiques visant à profiter de certaines tendances ou tout au moins de s'en protéger. Par ailleurs, la variété des mutations et des nouvelles menaces qui agitent le monde économique est l'un des facteurs dans lesquels il faut situer l'émergence du renseignement économique privé.

[14] Ces termes sont définis au point 3.2.

Prenant la parole en mai 2002 à un séminaire consacré au renseignement économique et au management des ressources humaines ([15]), l'amiral français Jacques Célerier, ancien commandant de la force navale française lors des opérations alliées en Bosnie-Herzégovine puis, jusqu'à l'été 2001 directeur de l'Institut des Hautes Etudes de Défense Nationale, décrit ainsi l'évolution de la situation. Pour l'amiral, la dernière décennie du XXème siècle a vu le monde subir de gigantesques bouleversements géopolitiques, technologiques et économiques. Les conflits internationaux ont changé de nature, avec la mondialisation de l'économie, la concurrence économique est devenue compétition voire affrontement ([16]), les nouvelles technologies, par les capacités qu'elles procurent, ont modifié la notion même de puissance.

Dans ce nouveau monde instable, mouvant et terriblement conflictuel, l'entreprise est devenue, à l'image des armées, un combattant qui doit se doter des nouvelles armes indispensables aux batailles qui l'attendent, et en premier lieu se donner les moyens de maîtriser l'information qui apparaît de plus en plus comme ressource essentielle, comme une matière brute sur laquelle repose à présent la puissance.

Ainsi, de même que le renseignement est absolument nécessaire à la connaissance de la situation sur laquelle le chef militaire fonde sa décision stratégique, l'intelligence économique est l'outil indispensable qui permet à l'entreprise de disposer des connaissances nécessaires à l'élaboration de sa stratégie.

Pour conclure, l'amiral Célerier estime qu'avec la fin de la Guerre froide, les conflits ont cessé d'être principalement politico-militaires pour devenir essentiellement économiques. Dès lors les pratiques de renseignement ont naturellement tendance à « s'exporter » en direction des entreprises qui sont devenues les acteurs de première ligne dans les nouveaux conflits géo-économiques. C'est sur base de cette idée que sont nées les notions de renseignement et d'intelligence économique qui ne prétendent pas se laisser assimiler à de l'espionnage économique, qui n'est lui, rien d'autre que du vol de données appartenant à une entreprise.

3.1.1. Le renseignement économique : affaire d'Etat ou affaire privée ?

A en croire donc l'amiral Célerier – et aussi de nombreux acteurs de ce marché -, le « renseignement privé » serait une réalité nouvelle, remontant à la fin de la guerre froide et à la chute du bloc soviétique.

Même si l'on ne peut nier que la fin de l'affrontement entre les blocs a accéléré une dynamique – entre autres par le simple fait que des milliers d'agents et officiers de renseignement se sont retrouvés sans emploi et ont bien été forcés de se recycler -, celle-ci préexistait à la fin du monde bipolaire. Plusieurs chercheurs et acteurs ([17]), parmi lesquels les experts du Comité R ([18]), ont d'ailleurs souligné, dans leurs travaux, que le renseignement privé n'était pas aussi neuf qu'on voulait bien faire semblant de le croire.

---

15 Cette journée d'étude à laquelle une membre du Comité permanent R a participé, était organisée le 22 mai 2002 conjointement par le CERAM de Sophia Antipolis et par l'Institut des Hautes Etudes de Sécurité Intérieure (IHESI).

16 C'est la notion de « guerre économique » développée par Christian Harbulot et Philippe Baumard dans « *Intelligence économique et stratégie des entreprises : une nouvelle donne stratégique* », Paris, 1996.

17 Notamment : Bernard Esambert, De la Guerre économique, in Revue Française de géo-économie, 1997 ; Genovefa Etienne et Claude Moniquet, *Histoire de l'Espionnage Mondial*, éditions Luc Pire et éditions du Félin, 2000 et 2002 ; Marc Borry et Frédéric Moser, *Intelligence stratégique et espionnage économique*, éditions Luc Pire et éditions de l'Harmattan, 2002.

18 Leur contribution au présent rapport est indiquée en lettres italiques.

Sans remonter jusqu'à l'Antiquité, ni même jusqu'au Moyen-âge ([19]), force est de constater que l'économie et l'industrie ont toujours constitué une matière intéressant les spécialistes de la collecte du renseignement et que, donc, avant que le renseignement d'Etat ne se professionnalise réellement et définitivement, à la fin du XIXème siècle, il existait bien des individus voire des compagnies spécialisées dans le renseignement privé. Ces structures privées se sont pourtant développées de manière inégale dans les différents pays, faisant de véritables efforts en matière d'acquisition de renseignement.

En résumé, l'essor du renseignement privé qui est en cours depuis plus de dix ans peut apparaître comme une nouveauté mais, observé sur le long terme, le phénomène marquant l'histoire récente du renseignement est plutôt sa nationalisation. Ainsi, en Belgique, ce n'est que tout à fait récemment que la protection du potentiel scientifique et économique du pays est devenue l'une des missions de la Sûreté de l'Etat. Par contre, le développement du secteur du renseignement privé n'est qu'un retour à l'état antérieur des choses.

Ce retour au renseignement privé se réalise sous l'effet de plusieurs facteurs prédominants : d'une part, la réduction progressive des budgets alloués aux agences nationales de renseignement, d'autre part, la mondialisation des menaces et la demande grandissante de renseignements de la part des entreprises et des décideurs économiques et enfin, la croissance quasi exponentielle des sources ouvertes et le développement des « Nouvelles Technologies de l'Information et de la Communication » (NTIC). Le développement des sources ouvertes et des NTIC n'est pas le moindre aspect de l'intrusion du secteur privé dans le monde du renseignement ([20]).

Pour l'avocat québécois Pierre Cloutier, « *le renseignement n'est pas et n'est plus l'apanage exclusif des Etats et des gouvernements Les grandes agences gouvernementales ne sont plus les seules à produire du renseignement et constitueront probablement même dans l'avenir des groupes minoritaires Le renseignement n'est pas non plus l'apanage exclusif des organisations privées ou publiques Avec le développement de ce que Winn Schwartau appelle le « Global Network », chaque individu deviendra non seulement un consommateur mais aussi un producteur de renseignement Le renseignement n'est plus relié exclusivement aux questions de sécurité nationale On assiste actuellement à une explosion sans précédent de nouveaux créneaux dans toutes les sphères de l'activité humaine. On parle désormais de renseignement d'affaires (business intelligence), de renseignement économique (economic intelligence), de renseignement diplomatique (diplomatic intelligence), de renseignement touchant le respect de la loi (law enforcement intelligence), de renseignement touchant la protection civile (operations other than war intelligence), de renseignement touchant au maintien de la paix (peacekeeping intelligence), de renseignement politique (political intelligence), de renseignement touchant l'environnement (environmental intelligence), etc. »* ([21])

Mais certains auteurs voient aussi dans le recours croissant au renseignement privé et dans la privatisation de la sécurité un phénomène permettant aux Etats de poursuivre à l'étranger des objectifs politiques, économiques et militaires de manière dissimulée. Selon les experts du Comité R : *« il est loin d'être exclu que soit déléguée à certains acteurs du secteur privé une partie des activités du secteur public. Ainsi, le privé pourrait intervenir en amont et en*

---

19 L'historien français Jean Favier a souligné, in *De l'or et des épices, naissance de l'homme d'affaires au Moyen Âge*, Fayard, 1987, l'importance pour les négociants du XIVème siècle de disposer de renseignements fiables, précis et rapides.

20 M. Robert Steele, un ancien du renseignement militaire des Etats-Unis milite depuis une dizaine d'année avec son association « *Open Sources Solution*» pour un recours massif à ces sources qui sont, selon lui, susceptibles de fournir l'essentiel des informations utiles aux entreprises sans qu'il soit nécessaire de recourir aux moyens dispendieux et dangereux du renseignement secret.

21 Pierre Cloutier "*Renseignement et sécurité dans l'âge de l'information : les défis du Québec*" (http://strategique.free.fr/analyses/rsai.pdf)

aval de l'action de l'Etat. En aval, il s'agirait de mener des opérations de renseignement et de guerre psychologique en appui à des politiques données dans des secteurs géographiques sensibles où dans des zones sur lesquelles il est exclu que des services d'Etat prennent le risque d'agir. Les Etats-Unis et la Grande-Bretagne ont, de longue date, compris l'intérêt de ce système qui permet de limiter les risques politiques inhérents à l'action clandestine et de réduire considérablement certaines dépenses récurrentes (entre autres de personnel) liées au travail du renseignement. En amont, le secteur privé pourrait devenir un fournisseur d'analyse de contexte, sur « sources ouvertes » dont les services de renseignement sont de grands consommateurs. Un autre secteur dans lequel les sociétés de renseignement privées pourraient se développer au profit des Etats est évidemment celui des manœuvres d'influence (lobbying). »

3.1.2. Le renseignement privé au service du développement des entreprises.

De plus en plus d'entreprises, sensibilisées à la valeur de l'Intelligence économique, ont implanté en leur sein une cellule de veille. D'autres ont recours à des cabinets spécialisés pour des cas précis et pour des durées déterminées généralement à l'avance. L'information stratégique à caractère technologique et concurrentiel s'est d'abord inscrite naturellement dans la culture des entreprises du secteur de la défense et de l'armement. Dans ce premier cas, il s'agissait surtout de veille concurrentielle ou technologique, ce qui ne constituait pas encore à proprement parler de l'Intelligence économique.

Ensuite, on a vu apparaître dans l'organigramme d'autres entreprises multinationales, notamment chez les industriels de l'agroalimentaire, des secteurs énergétiques (pétrole, nucléaire), des compagnies aériennes, etc., des cellules de décisions appelées *war rooms*. Il s'agit de lieux où l'on rassemble toute l'information utile à la prise de décision dans le cadre d'un projet particulier ou d'une stratégie spécifique mise en place par l'entreprise. Ces cellules sont chargées de gérer les crises, de répondre aux conséquences d'accidents industriels de plus en plus fréquents, de contrer les attaques de la concurrence, mais aussi de maîtriser l'information à caractère stratégique de l'entreprise et de s'attaquer à la conquête de nouveaux marchés. Certaines de ces *war rooms* sont animées par d'anciens membres de services de police ou de renseignement. Parmi les pratiquants du renseignement ou de l'Intelligence économique, on trouve à présent des petites et moyennes industries (PMI) et des petites et moyennes entreprises (PME).

Mais pour Messieurs Besson et Possin ([22]), les acteurs de l'intelligence économique au sein de l'entreprise ne doivent pas devenir des professionnels du renseignement et l'adhésion au projet ne doit pas les entraîner sur des chemins incertains, voire dangereux et illégaux. C'est pourquoi ces auteurs recommandent de sous-traiter sans honte, en dehors de l'entreprise, aux professionnels de l'intelligence économique et du renseignement commercial, les questions difficiles. En matière de renseignement, la sous-traitance tend en effet à se généraliser. Les entreprises y ont recours soit parce qu'elles ne disposent pas des capacités internes pour traiter ce genre de dossier, soit parce qu'elles ne maîtrisent pas les sources, par manque de temps ou de motivation du personnel ou enfin par souci de confidentialité et de cloisonnement. Rares sont en effet les entreprises qui admettent ouvertement pratiquer le renseignement économique.

[22] Besson & Possin, "*Du renseignement à l'intelligence économique*" Dunod – Paris 1996

On trouve depuis quelques années des rapports officiels ainsi qu'une abondante littérature consacrée à l'intelligence économique et à certaines pratiques connexes comme la veille stratégique ou concurrentielle, le « *Benchmarking* », la « *Corporate Intelligence* », l'« *Investigative Due Intelligence* » et autres disciplines aux noms anglo-saxons. On y décrit généralement l'espionnage comme une pratique illégale, par opposition à l'Intelligence économique qui serait légale. Les définitions données à ces notions sont multiples.

L'intelligence économique devient donc une discipline autonome et un art dont les promoteurs travaillent soit au sein d'un service spécifique de leur propre entreprise, soit au sein de sociétés privées spécialisées qui constituent une nébuleuse hétérogène aux formes juridiques très variables. L'intelligence économique est aussi devenue un marché obéissant aux lois de l'offre et de la demande ([23]). Au cœur des guerres commerciales, le renseignement est devenu un produit qui se vend et qui s'achète, donnant lieu à la création de dizaines de sociétés nationales ou de cabinets aux effectifs modestes, mais aussi d'entreprises multinationales employant plusieurs centaines de personnes et gérant, à travers le monde des réseaux d'experts. Des Hautes Ecoles publiques ou des Instituts privés dispensent à présent des formations très pointues en ce domaine.
Pourtant, il apparaît encore que l'Intelligence économique ne jouit pas partout d'une grande estime auprès des grands patrons, notamment en France où les cabinets spécialisés en la matière semblent éprouver des difficultés à en vivre. La situation des cabinets français est donc radicalement différente de celle des cabinets britanniques ou américains, dont les compétences sont reconnues et utilisées par les gouvernements. Ce monde des sociétés et des cabinets d'intelligence économique est donc fort disparate, selon les pays, et en constante évolution. Les matières ne sont pas assises sur un socle définitif et le concept d'Intelligence économique n'est d'ailleurs pas encore défini avec précision. Il convient donc d'éviter de donner aux sociétés ainsi désignées une définition trop formelle.

3.1.3. Le renseignement privé au service de la sécurité des entreprises.

Les attentats du 11 septembre 2001 et plus récemment celui de Karachi le 8 mai 2002, où onze ingénieurs navals français furent tués par une voiture piégée, ont rappelé aux responsables économiques que dans un monde globalisé, l'entreprise et ses collaborateurs peuvent se trouver au cœur de crises politiques, ethniques ou sociales qui les impliquent malgré eux. Ces évènements ont, de manière prévisible, provoqué une très forte augmentation de la demande de dispositifs de sécurité physique des entreprises, particulièrement les entreprises américaines. Par ailleurs, une enquête parue dans le n° 42 (28/03/2002) du bi mensuel « *Intelligence On Line* » semble aussi indiquer une forte augmentation de la demande sécuritaire des grandes entreprises à l'égard des professionnels du renseignement économique.

[23] Plusieurs documents permettent d'avoir une vision globale de ce marché du renseignement économique. Pour la France, il existe notamment un "*Annuaire Européen des Professionnels de l'Intelligence Economique*" édité en 1998 par la "*Société d'Intelligence Economique et Concurrentielle Appliquée*" (SIECA). Ce manuel n'a pas été réédité, ni mis à jour, de sorte qu'il paraît dépassé à ce jour. Voir aussi *« France : le top 100 de l'intelligence économique Intelligence On Line reports » Editions Indigo Publications, Paris 2004.* Le site Internet www.seymourab.com/intelligence.htm présente une série de liens avec des sites d'agences officielles ou privées de renseignement.

Dans les mois de crise qui ont suivi les attentats, les responsables de l'intelligence économique de plusieurs grands groupes se sont inquiété des risques encourus par leurs sociétés dans certains montages financiers impliquant des hommes d'affaires réputés proches des milieux islamistes. A la publication de chaque nouvelle liste du Département américain du Trésor énumérant les personnes et les banques soupçonnées de financer le terrorisme islamiste, les firmes de renseignement économique ont été chargées de rechercher les partenaires d'affaires de tous les individus et de toutes les structures citées. De nombreuses entreprises ont également sollicité des enquêtes de sécurité (*background check)* sur les membres de leur personnel.

De multiples cabinets de renseignement économique se sont donc tournés vers la sécurité et le contre-terrorisme pour proposer à des entreprises ou à des collectivités locales des audits sur leur vulnérabilité aux attaques terroristes.

3.1.4. Qu'est-ce qu'une société de renseignement privée ?

Selon l'IHESI (Institut français des Hautes Etudes de la Sécurité Intérieure ([24]) le terme générique de Société de Renseignement Privée (SRP) désigne des sociétés dont l'activité réelle, déclarée ou parfois masquée sous celle plus générale de conseil en sécurité, est la recherche d'informations pour compte de tiers.

La loi française du 18 mars 2003 pour la sécurité intérieure ([25]) définit de la manière suivante les « *activités des agences de recherches privées* » : il s'agit d'une « *profession libérale qui consiste, pour une personne, à recueillir, même sans faire état de sa qualité ni révéler l'objet de sa mission, des informations ou renseignements destinés à des tiers, en vue de la défense de leurs intérêts ».*

Ces définitions sont extrêmement larges puisqu'elles englobent tout type de recherche d'informations ou de renseignements, effectuée pour le compte de tiers et dans leur intérêt, quel que soit la nature des informations recherchées et leurs finalités (informations à caractère privé, économique, de sécurité, etc.) L'activité des cellules de renseignement dont certaines entreprises se sont dotées n'est donc pas visée par la loi française aussi longtemps qu'elle s'effectue pour l'entreprise elle-même et pas pour le compte de tiers.

3.2. Aperçu de prestations disponibles en rapport avec le renseignement privé.

Plusieurs catégories de prestations, en rapport direct ou indirect avec le renseignement économique ou de sécurité, sont proposées par des firmes privées. Ces sociétés privées d'investigation et de sécurité suivent en effet les mêmes évolutions que les grands cabinets d'audit. Elles élargissent leur gamme de services, s'affranchissent des limites de leur métier d'origine et opèrent de multiples fusions, acquisitions ou séparations, d'où de fréquents mélanges de genres au sein de firmes de conseil et d'expertises comptables et juridiques.

---

[24] Créé en 1989, l'Institut des Hautes Etudes de la Sécurité Intérieure (IHESI) est placé sous l'autorité directe du ministre français de l'Intérieur.

[25] Article 20 de la loi n° 83-629 du 12 juillet 1983 réglementant des activités privées de sécurité, créé par la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure (http://www.legifrance.gouv.fr/). Il sera encore question plus loin de cette loi française.

Elles proposent donc en parallèle des services proches, plus porteurs, comme l'expertise comptable et l'audit de management, la consultance en stratégie et le lobbying. On s'éloigne alors de la problématique du renseignement ou de l'Intelligence économique.

Le présent rapport s'attardera sur quelques activités productrices ou consommatrices de renseignements telles que :

- le recueil et la production de renseignement à caractère économique et commercial ;
- les différents types de veille, technologique, concurrentielle (ou *benchmarking*), stratégique ou juridique ;
- l'intelligence économique ;
- l'intelligence sociale ;
- l'influence et le lobbying ;
- l'intermédiation dans la négociation de contrats internationaux;
- la guerre et la contre-guerre de l'information ;
- la surveillance des systèmes informatiques (ou Cyber-surveillance) ;
- les enquêtes de sécurité préalable à l'engagement de cadres et de dirigeants d'entreprises (« *Pre Employment Screening* »;
- l'analyse des « risques pays » ;
- l'expertise comptable et l'audit de management ;
- le gardiennage de sécurité ;
- le renseignement « humanitaire » ;
- le renseignement « militant » ;
- le renseignement militaire privé.

3.2.1. Le renseignement économique et commercial

On entend par renseignement économique toutes les informations économiques à caractère politique ou commercial, y compris les données technologiques, financières, commerciales en propriété exclusive, ainsi que les informations gouvernementales, qui sont susceptibles de contribuer directement ou indirectement à l'accroissement de la productivité ou à l'amélioration de la position concurrentielle des puissances étrangères qui en font l'acquisition ([26]).

Le renseignement commercial : une véritable industrie de l'information professionnelle émerge depuis une quinzaine d'années, donnant naissance à une nouvelle profession : celle d'intermédiaire (ou courtier) en informations (*broker* en anglais). Dans la terminologie anglo-saxonne, on désigne souvent cette discipline par les vocables « *Corporate Intelligence* » ou « *Investigative Due Intelligence* ». Sur ce marché, la demande provient essentiellement, mais non exclusivement, des entreprises qui veulent s'assurer lors de la signature d'un contrat de la solvabilité de leur client.

[26] "Série d'aperçus" n° 6 - mai 1998, publication du Service canadien de Renseignement de Sécurité.

Le « risque client » représenterait 90 % des demandes de renseignements adressées aux professionnels de ce secteur. Les entreprises constituent la majorité des demandeurs de renseignements, mais d'autres donneurs d'ordres apparaissent comme les avocats, les collectivités locales (en France, du moins), les syndicats patronaux ou de travailleurs désireux de se renseigner sur la santé commerciale de leurs partenaires ou de leurs employeurs. Des sociétés de renseignement commercial ou autres ont constitué d'importantes bases de données puisées auprès de sources ouvertes et officielles, telles que les greffes des tribunaux de commerce, les rapports et bilans de la Banque nationale, la presse, etc. Les sociétés de renseignement les plus performantes ont su tisser des réseaux dépassant les frontières et obtenir l'accès à des informations « fermées » ou orales. Ces données ainsi rassemblées permettent de dresser des dossiers sur un bon nombre d'entreprises, sur leurs actionnaires et dirigeants, leur patrimoine, leurs clients, leur personnel, leur chiffre d'affaire, leur solvabilité ou leur situation d'endettement. Des biographies d'hommes et de femmes d'influence ainsi que des organigrammes complets de ministères et d'administrations sont également disponibles par pays.

Il existe aussi des banques de données sur les entreprises publiées sous forme d'annuaires et de catalogues ([27]), également accessible au grand public via des sites web sur l'Internet moyennant paiement ([28]) régulièrement enrichies et remises à jour en temps réel. A la demande de clients, de véritables dossiers historiques, économiques et financiers peuvent être constitués sur telle ou telle entreprise, contenant aussi des données administratives (raison sociale, statuts et forme juridique, etc.).

Certaines firmes apportent une valeur ajoutée à ces informations qu'elles délivrent en produisant des analyses plus ou moins circonstanciées et actualisées ainsi qu'en émettant des avis sur le « risque » encouru lors de projets de contrats ou de rachats d'entreprises. Ces avis peuvent prendre la forme d'une cotation du risque sur une échelle allant de 0 à 20 et qui s'appelle le *scoring.* Celui-ci se fonde sur des critères d'analyse plus ou moins objectifs qui sont propres à la société de renseignement, mais aussi sur le sentiment de l'analyste, rédacteur du rapport, qui peut aussi prendre en considération des critères plus arbitraires comme l'implantation géographique de l'entreprise dans une zone défavorisée ou sinistrée économiquement, l'âge des dirigeants, les conflits sociaux ou la structure de son bilan, etc.

Les sociétés de renseignement commercial vivent dans une concurrence exacerbée. Certaines d'entre elles s'engagent à ne pas servir la concurrence étrangère au détriment de leurs clients nationaux. Ces sociétés de renseignement commercial deviennent ainsi les auxiliaires précieux de groupes internationaux désireux d'acquérir au bon moment et au plus juste prix des PME à la recherche de repreneurs. Les PME les plus performantes, celles disposant de savoir-faire reconnus ou de technologies les plus avancées, sont la cible de ces groupes étrangers qui peuvent alors réaliser le plus légalement du monde des transferts de technologies avant que celles-ci ne soient protégées par le dépôt d'un brevet.

Certaines firmes éditent des rapports d'analyse de risques plus généraux mais qui contiennent néanmoins des informations pointues et précises pour les industriels qui désirent investir à l'étranger. Il s'agit de rapports portant sur la situation politique, sociale et économique des pays visés, sur les intérêts des groupes rivaux, sur les menaces terroristes, les pratiques de corruption, sur l'influence des groupes criminels ou celle des groupes de pression, comme par exemple celui intitulé "*2000 Outlook"* de la firme *"Control Risks Group".*

[27] Pour la Belgique, voir par exemple l'annuaire "*Top 30.000*" en version livre publié par *Trends - tendances* et le « *Top 100.000* » en version CD.

[28] Exemples de sites : http://societe.journaldunet.com , www.transnationale.org , www.dnb.com , http://www.spectron.be/ , www.strategic-road.com/club , etc.

Le coût du renseignement commercial dépend du contrat ou de l'abonnement passé entre l'entreprise et la société de renseignement. Il se calcule en fonction « d'unités d'accès » aux banques de données gérées par celle-ci et varie selon les extraits sollicités. Par exemple, les rapports commerciaux et financiers proposés par Trends-Tendances coûtent environ 40 € par entreprise. Le renseignement à la carte exige une enquête plus poussée dont le coût varie en fonction des questions posées et du degré de difficulté rencontré pour obtenir l'information sollicitée.

3.2.2. La veille

Les concepts de veille et d'intelligence économique ne sont pas figés. Ils sont en constante évolution. La veille en général peut se définir comme la mise en œuvre de dispositifs récurrents et méthodiques pour collecter, traiter, diffuser et suivre l'information utile. La veille est le concept précurseur de l'intelligence économique dans l'entreprise. Il s'agit pour l'entreprise de se constituer une documentation grâce à l'utilisation d'instruments d'accès à des banques de données, à des systèmes de traitement automatisé de ces données et des outils d'analyse de l'information. Ces données entrent dans le système de veille et il en ressort des renseignements utiles à la prise de décisions stratégiques, notamment en matière de Recherche et Développement et de transferts de technologies. Ayant dépassé l'aspect purement technique et scientifique, le concept de veille s'est progressivement étendu à d'autres domaines d'informations pour devenir plus global. La veille est désormais multiforme, on en distingue plusieurs types :

- **La veille technologique** consiste en une surveillance des informations ayant trait aux recherches scientifiques, aux techniques de pointe ou aux nouveaux procédés de fabrication. Elle s'intéresse aux évolutions technologiques (incluant la recherche scientifique et les produits mis sur le marché) susceptibles d'influer sur le devenir du secteur d'activités en vue d'appuyer la prise de décision quant aux investissements futurs de l'entreprise. La veille technologique inclut l'observation et l'analyse de l'environnement scientifique, technique, technologique et économique de l'entreprise pour en détecter les menaces et saisir les opportunités de développement. Divers types d'informations sont pris en compte : scientifique, technique, (avec une importance considérable de l'information contenue dans les brevets) et technologique.

- **La veille concurrentielle** s'intéresse aux concurrents actuels ou potentiels, aux nouveaux entrants sur le marché qui peuvent notamment apparaître avec des produits de substitution. Dans ce type de veille, on distingue également le **benchmarking** qui consiste à observer ce que les concurrents font de mieux dans le secteur. C'est ainsi qu'une entreprise peut se remettre en question pour progresser. Le benchmarking est une discipline qui permet à une entreprise de se comparer à ses concurrents ; elle s'intéresse non seulement aux produits et au marché, mais aussi à l'ensemble de la gestion et de la production, à la recherche et développement, aux chiffres d'affaires, aux brevets et innovations, aux produits, méthodes et coûts de production ainsi qu'aux circuits commerciaux et de marketing. Cette veille s'attache à découvrir des faits dont l'analyse permet de dégager des tendances à venir afin de pouvoir les anticiper.

- **La veille commerciale** consiste en une surveillance des informations relatives à l'environnement commercial de l'entreprise. Elle concerne les marchés, les appels d'offre, les clients et les fournisseurs. Au delà des études de marketing, il s'agit de s'intéresser à l'évolution des besoins des clients sur le long terme ou encore de retrouver rapidement une source d'approvisionnement en cas de défaillance d'un fournisseur.

- **La veille juridique** constitue une nouvelle spécialité sectorielle de la veille en général. Elle s'attache à suivre régulièrement et de manière rigoureuse la législation, la jurisprudence, les règlements nationaux, les directives européennes et les traités internationaux pour éviter d'être surpris par les évolutions en la matière, de mener des actions de lobbying ou même de prendre les devants afin d'obtenir un avantage concurrentiel. Le droit et ses applications sont ici envisagés en tant qu'information susceptible d'influencer l'évolution des marchés économiques. Parmi les méthodes utilisées, on relève l'inventaire des instruments juridiques tels que les brevets et les marques déposées ou encore le suivi de contentieux impliquant la concurrence ([29]). Se tenir informé sur les projets législatifs et de conventions internationales en cours de discussion peut permettre d'anticiper une modification de l'environnement juridique et de s'y adapter ou le cas échéant, de déclencher une stratégie d'influence ou de lobbying.

- **La veille environnementale** englobe d'autres secteurs d'observation tels que le champ politique, social, culturel, etc. On voit aussi apparaître le concept de **veille sociétale** tendant à capter les nouvelles tendances émergentes dans les comportements sociaux. Cette discipline intéresse surtout les sociologues et les spécialistes du marketing.

- **La veille stratégique** regroupe l'ensemble des différentes veilles ; elle constitue un processus d'aide à la décision qui vise à observer et à analyser l'ensemble des informations présentes dans l'environnement de l'entreprise en vue de définir ou d'infléchir la stratégie de l'entreprise.

De nombreuses firmes commerciales, associations professionnelles, parfois en association avec des collectivités territoriales ou des pouvoirs régionaux, organisent pour des cadres d'entreprises des séminaires de formation à la veille technologique, concurrentielle, économique ou autre ([30]). Au cours de ces séminaires de formation, on peut apprendre à mettre en place une surveillance automatique de ses concurrents, par exemple en développant une méthode d'interrogation sur Internet basée sur de puissants moteurs de recherches, en tirant parti de la «zone grise» d'Internet et des informations cachées qui s'y trouvent, en apprenant à surfer sur le Net en laissant le moins de traces possibles, etc.

3.2.3. Le renseignement économique et l'intelligence économique.

Le **renseignement économique** et **l'intelligence économique** sont deux notions complémentaires mais distinctes qui ne veulent pas se laisser assimiler à de l'espionnage économique.

On entend par **renseignement économique** toutes les informations économiques à caractère politique ou commercial, y compris les données technologiques, financières, commerciales en propriété exclusive, ainsi que les informations gouvernementales, qui sont susceptibles de contribuer directement ou indirectement à l'accroissement de la productivité ou à l'amélioration de la position concurrentielle des puissances étrangères qui en font l'acquisition ([31]).

---

29 Bertrand Warusfel, *L'intelligence économique et de droit,* Cahiers de la fonction publique et de l'administration, novembre 1995, cité par Jérôme Dupré dans *Renseignement et entreprises,* Lavauzelle, 2002.

30 Voir par exemple les séminaires organisés par SCIP France (www.scip-France.org) ou par *l' « Institute for International Research »* (www.iventis.fr). En Belgique, des séminaires desensibilisations à la veille sont organisés par la Chambre de Commerce et d'Industrie du Hainaut et par le Bureau économique de la province de Namur (voir plus loin).

31 "Série d'aperçus" n° 6 - mai 1998, publication du Service Canadien de Renseignement de Sécurité

L'intelligence économique ([32]) peut être définie de plusieurs manières.

Le professeur Stevan Dedijer fut l'un des premiers universitaires à avoir formalisé l'intelligence économique dans les années 70 à l'université de Lund (Suède) ; il estime que cette discipline doit avoir pour rôle de nourrir les "*intuitions des décideurs*".

En France, on la considère généralement comme l'ensemble des actions coordonnées de recherche, de veille, de traitement et de distribution, en vue de son exploitation, de l'information utile aux acteurs économiques ([33]).

Le renseignement économique et l'intelligence économique sont donc deux notions complémentaires mais cependant distinctes. Le concept plus large d'intelligence économique regroupe l'ensemble des différentes veilles mais s'en distingue par l'emploi de méthodes plus actives de recueil du renseignement. L'intelligence économique a pour vocation de rechercher et de détecter dans son environnement proche ou lointain les menaces et les opportunités de toute nature auxquelles l'entreprise doit faire face, ceci dans un contexte de concurrence exacerbé :

- détecter les menaces suppose une attitude défensive que l'entreprise doit développer pour protéger son patrimoine, ses brevets et ses connaissances ;
- détecter les opportunités de développement suppose une attitude plus offensive pour survivre par l'innovation et la diversification dans un monde en constante mutation.

Instrument d'analyse, l'intelligence économique valide l'information utile et anticipe sur toutes les stratégies possibles, elle combat la désinformation, tire des leçons des erreurs passées et des dysfonctionnements de l'entreprise. A l'occasion, elle permet de découvrir des fraudes et des trahisons internes.
Mais certains n'hésitent pas à présenter l'intelligence économique comme une utilisation efficace de l'information à travers des activités de lobbying et d'influence, voir même de corruption. Une équipe française de recherche associée au Centre des Hautes Etudes de l'Armement (CHEAr) estime que "*parce que la concurrence ne s'assimile pas à la guerre, le renseignement économique n'est pas une forme de renseignement comme les autres. En effet, il utilise essentiellement des méthodes ouvertes et ses multiples acteurs sont autant publics que privés. Plus qu'un espionnage économique inadapté, le véritable enjeu est de créer un réseau d'intelligence économique, favorisant la diffusion de l'information au sein de l'économie nationale et dépassant certains travers culturels tels que la rétention d'informations"* ([34]).

Certains auteurs estiment que l'intelligence économique, selon qu'elle est pratiquée par les entreprises ou les Etats, n'obéit pas toujours à la même logique dans les deux cas. Et ceux-ci de développer le tableau suivant ([35]) :

---

[32] A la fois anglicisme et néologisme, cette expression peut prêter à confusion par la double acception du mot anglais « intelligence » ; elle est pourtant préférée par de nombreux francophones au terme français "renseignement économique", car elle leur paraît mieux refléter la richesse de cette activité et l'étendue des connaissances et de la culture qu'il met en oeuvre.

[33] Rapport du 10ème plan français (février 1994) "*Intelligence Economique et stratégique des entreprises*" (souvent désigné sous l'appellation "rapport Martre").

[34] "*Le renseignement économique : enquête sur un faux débat"* - Nicole Chaix, Philippe Dubost, Arnaud Voisin dans "Les cahiers de la sécurité intérieure" n° 30 1997 - IHESI

[35] D'après "*une approche française de l'intelligence économique"* - Christian Harbulot - 1995

L'intelligence économique	des entreprises	des Etats
a pour objectif final :	le développement de l'entreprise,	la puissance économique,
cible :	les produits,	le marché mondial,
recherche d'abord :	l'information centrée sur les métiers,	l'information centrée sur les réseaux,
pratique :	le lobbying,	l'influence,
recherche l'information :	dans le marché privé de l'information,	dans le processus du renseignement,
transmet l'information :	au PDG, au conseil d'administration,	à l'autorité politique responsable de l'économie
est imprégnée :	de la culture d'entreprise,	de la culture du renseignement.

Dans la réalité, la pratique de l'intelligence économique par les entreprises et celle des Etats ne sont probablement pas aussi clichées que le voudraient ces auteurs. Le Comité permanent R retiendra pour sa part que les objectifs de l'intelligence économique pratiquée par les entreprises ne coïncident pas toujours avec la préservation de la puissance économique de la Nation.

3.2.4. L'intelligence sociale.

Ce secteur particulier de l'intelligence économique et stratégique s'intéresse plus particulièrement au suivi des rapports humains dans l'entreprise. Il s'agit le plus souvent d'activités d'investigations et de prospective sur les mouvements syndicaux. Il existe en France une petite catégorie d'experts de ce champ d'observation. A Paris, cette discipline est enseignée à l'Institut des Hautes Etudes de la Défense Nationale dans le cadre de son cycle de cours sur l'intelligence économique.

3.2.5. La surveillance des systèmes informatiques (ou Cyber-surveillance).

Depuis plusieurs années, la criminalité et la délinquance évoluent avec les nouvelles technologies. De nombreux délits peuvent être perpétrés à partir de n'importe quel point du globe vers un autre grâce au réseau Internet et à l'aide d'un ordinateur : vols d'informations confidentielles, détournement de courrier électronique, destructions ou modification de données, chargement de virus, propagation de fausses rumeurs, d'appel à la haine raciale, etc. La multiplication des réseaux informatiques sans fil accroît aussi ces nouveaux risques pour les utilisateurs. Certains se servent d'ailleurs de ces moyens pour accomplir leurs forfaits en ne laissant sur l'Internet que la trace de l'ordinateur dont ils ont volé l'identité. Ces risques sont d'autant plus dangereux que la menace est souvent invisible.

La sécurité informatique, combinée à une stratégie de défense de l'information stratégique et de protection de l'entreprise, devient donc une discipline globale dans l'organisation des entreprises. Le marché de la sécurité et de la surveillance des systèmes informatiques explose donc en conséquence.

De nombreuses firmes et consultants privés offrent donc des services de vérification des niveaux de sécurité dans les systèmes d'information des entreprises et leur prodiguent des conseils pour les aider à les renforcer. A cet effet, certains n'hésitent pas à recourir à des techniques de *hacking* pour tester les vulnérabilités des équipements matériels ou des logiciels composant le système d'information de leur client.

Par ailleurs, de nouvelles techniques d'investigation sont apparues destinées à détecter les actes de criminalité informatique ou à en identifier les auteurs. Des firmes produisent et utilisent des logiciels de surveillance qui permettent d'enregistrer tous les évènements survenus sur un ordinateur et toutes les actions de son utilisateur : les frappes sur le clavier, les dates et heures d'ouverture et de fermeture d'une session, les programmes utilisés, les sites web consultés, les documents créés, consultés ou supprimés, etc. Des programmes sont conçus pour détecter la présence de logiciels espions dans un système informatique.

Des programmes sont aussi utilisés pour permettre une nouvelle forme de surveillance du personnel sur les lieux de travail. L'on voit en effet des grandes firmes mettre en place des dispositifs électroniques internes chargés d'enregistrer les déplacements internes du personnel pourvu de badges, de surveiller les consultations du réseau Internet, le contenu des disques durs, des communications téléphoniques ou des messages électroniques de leurs salariés, parfois à leur insu et dans le but de trouver, soit d'éventuelles fautes commises au travail, soit des preuves informatiques de fraudes ou de vols de secrets industriels. D'après une étude réalisée en Grande Bretagne, 20 % des entreprises surveilleraient le courrier électronique de leurs employés et leurs consultations du Web. Les abus en ce domaine constitueraient même aujourd'hui le principal motif de sanctions au sein des sociétés britanniques.
Les législations américaine et britannique permettent en effet aux employeurs de recourir à cette *"médecine légale informatique"* qu'ils justifient par la nécessité de protéger le patrimoine de l'entreprise et de lutter contre la diffusion de secrets industriels.

En Belgique, toute mise en place d'un contrôle doit être discutée au conseil d'entreprise puis affichée ou, à défaut, être communiquée à chaque travailleur. [36] Certaines entreprises ont inclus un code de bonne conduite pour l'usage du courrier électronique ou la consultation du réseau Internet.

La Commission pour la protection de la vie privée a déjà exprimé à trois reprises sa vision des choses sur la légitimité du contrôle des messages électroniques échangés entre employés (avis n° 10/2000 du 3 avril 2000 ; avis n° 39/2001 du 8 octobre 2001 et avis n° 13/2003 du 27 février 2003).

La Commission souligne qu'il existe de nombreuses dispositions légales, d'ordres divers, à prendre en considération dans cette matière. Il s'agit principalement de l'article 8 de la CEDH et de l'article 22 de la Constitution, des articles 4 et 5 de la loi sur la protection des données à caractère personnel, de l'article 109 ter D de la loi Belgacom et de l'article 6 de la loi du 8 avril 1965 sur les règlements de travail.

[36] Voir la Convention collective de travail n° 81 du 26 avril 2002 "relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électronique en réseau" rendue obligatoire par l'Arrêté royal du 12 juin 2002 (M.B. du 29 juin 2002).

Il ressort clairement de ces règles qu'un employeur ne peut pas contrôler arbitrairement les messages électroniques de ses employés. Le droit à la protection de la vie privée vaut aussi sur les lieux de travail. Il appartient donc aux employeurs et aux salariés de chercher ensemble comment établir un équilibre entre le contrôle et la protection de la vie privée. Cette recherche doit se faire en fonction des circonstances concrètes du travail (notamment la nature du travail lui-même et de son environnement, la nature des responsabilités). Les diverses législations (parfois très contraignantes) ne peuvent être transgressées. Le contrôle des communications sur les lieux du travail doit satisfaire aux exigences de la transparence, de la proportionnalité et de la nécessité ; un tel contrôle doit rester l'exception et sa justification ne peut être justifié par des finalités formulées en termes généraux. La Commission estime que toute prise de connaissance du contenu de messages envoyés par des salariés est injustifiée et excessive. La Commission émet encore davantage de réserves à l'égard du contrôle du courrier entrant.

3.2.6. Les enquêtes de sécurité préalable à l'engagement de cadres et dirigeants d'entreprises

(« *Pre Employment Screening* », « *Background Check-Up* » ou « *Background screening* »).

Des grandes entreprises ont pris le pli de faire examiner à la loupe le passé des candidats qui se présentent à certains de leurs postes clés. Avant de prendre une décision d'engagement, elles font procéder à des enquêtes sur la vie professionnelle et personnelle des postulants. Ces enquêtes visent notamment à vérifier l'intégrité et les compétences professionnelles du candidat, mais aussi son état de santé, son éventuelle dépendance à la drogue ou à l'alcool, ses faiblesses éventuelles, etc.

Ces enquêtes sont le plus souvent menées sans que la personne concernée n'en ait été avisée et a fortiori sans que son accord préalable n'ait été sollicité. Ces missions sont généralement confiées à des détectives privés. Ceux-ci consultent notamment des bases de données judiciaires et commerciales tenues par des firmes de renseignement commercial, mais ils procèdent aussi à de véritables investigations dans l'entourage familial et dans le milieu professionnel de la personne concernée. Il s'agit en sorte d'enquêtes fort similaires à celles que mènent les services officiels en vue de la délivrance d'une habilitation de sécurité.

En Belgique, ce type d'enquête est visée par l'article 1er, 2° de la loi du 19 juillet 1991 organisant la profession de détective privé qui vise le recueil d' « *informations relatives à l'état civil, à la conduite, à la moralité et à la solvabilité de personnes* ».

La « collecte de données à caractère personnel », par exemple par un détective travaillant pour le compte d'un employeur, relève donc aussi de la loi sur le traitement des données à caractère personnel en cas d'utilisation d'un procédé automatisé (par ex : prendre des photos numériques).

Mais même en l'absence de recours à un procédé automatisé (par ex : une enquête de voisinage), cette loi sera d'application si les données obtenues sont destinées à être enregistrées dans un « fichier ».

La question de savoir ce qu'il faut entendre au juste par « fichier » reste un sujet de discussion pour la doctrine. Si la loi sur le traitement de données à caractère personnel est d'application, l'intéressé peut naturellement prétendre à tous les droits résultant de cette loi.

Il pourra ainsi demander à être informé de ce qui se trouve dans son « fichier » (art. 10) et demander la rectification des données erronées (art. 12). Si cette loi n'est pas d'application, il n'existe aucune base pour contraindre l'employeur à communiquer les données.

En ce qui concerne spécifiquement la situation du candidat, l'on peut faire également référence à l'article 11 de la Convention collective de travail n° 38 du 6 décembre 1983 qui contraint l'employeur à respecter la vie privée du candidat. Cette convention collective de travail a pour objectif de fixer des normes concernant le recrutement et la sélection de travailleurs et de définir les engagements des parties signataires quant au respect d'un certain nombre de règles de conduite.

3.2.7. La sécurité des entreprises et des salariés à l'étranger.

L'attentat de Karachi, qui en mai 2002 a coûté la vie à onze ressortissants français, membres du personnel de la Direction des constructions navales (DCN), a mis en évidence la question de la sécurité des expatriés européens dans des zones instables de la planète.

Des firmes privées ou semi-publique se créent aux Etats-Unis et en France afin d'offrir une assistance sécurité aux entreprises qui envoient certains de leurs collaborateurs en mission dans des pays « à risques ». L'objectif est d'assister l'entreprise dans la résolution de cas critiques dépassant sa compétence ou ne relevant pas de son métier : enlèvement, extorsion de fonds, racket, chantage, détention arbitraire, acte de piraterie, crise sociale, situation insurrectionnelle, etc.

Les prestations de ces firmes s'articulent autour de la prévention des risques, l'assistance opérationnelle et la gestion des crises.

Le premier service offert est d'abord la production d'analyses *« risques pays* » portant sur la situation politique, économique et sociale de ces pays, accompagnées d'une évaluation des risques de sécurité encourus par les expatriés. De véritables audits de sécurité sont proposés analysant la sûreté et la vulnérabilité de certains sites d'implantation, d'hôtels, de prestataires de services ou indiquant le degré de fiabilité des autorités locales, etc.

La prévention s'organise ensuite, avec l'élaboration de plans de prévention et la diffusion de consignes de sécurité, l'élaboration de schémas directeurs de maîtrise et de gestion des risques, destinées aux cadres d'entreprises appelés à s'expatrier.

Enfin, l'assistance opérationnelle est proposée en vue de décharger la direction d'une entreprise de toute préoccupation liée à la sûreté sur le site à l'étranger. Cette assistance prend la forme de préparations de voyages d'affaires, d'interface avec les partenaires locaux et les autorités, de rédaction de cahiers de charges, d'appels d'offres, de sélection de fournisseurs, de contrôles des dispositifs de sécurité et de mise en œuvres de plans d'évacuation en cas de crise. Certaines firmes déclarent toutefois qu'elles s'abstiennent d'intervenir en temps de guerre.

3.2.8. Autres types de prestations proches du renseignement.

On aurait tort, selon les experts du Comité R, de penser que la collecte du renseignement concurrentiel ou économique est le seul domaine dans lequel des entreprises privées puissent avoir recours à des techniques « spéciales » de recherche d'informations. Par ailleurs, des entreprises de renseignement privé se dissimulent parfois sous d'autres vocables et d'autres métiers que ceux de « société ou d'agent privé de recherche ».

Dans le contexte de « guerre économique » qui s'est développée depuis une dizaine d'années dans le monde industrialisé, des sociétés privées ou des officines peuvent également être utilisées à d'autres fins comme le lobbying, la négociation plus ou moins occulte de contrats internationaux, la surveillance du personnel, la lutte contre la fraude et le vol, le contre-espionnage économique ou encore la réaction à des opérations d'atteinte à l'image et de dénigrement, dirigées contre des entreprises.

Dans la plupart des cas, les personnes, sociétés ou officines susceptibles de se livrer à ces opérations seront également en mesure de se livrer au renseignement privé.

D'autres prestations sont encore offertes par des sociétés qui gravitent aux marges du renseignement privé. Il s'agit par exemple des sociétés d'affacturage (firmes spécialisées dans le recouvrement et le contentieux qui gèrent aussi les comptes clients d'une entreprise - en anglais : *factoring),* des sociétés d'assurance-crédit, de courtage ou de fournisseurs de logiciels destinés à prévoir les risques du crédit aux entreprises.

La place des cabinets d'audit et d'expertise comptable dans le monde du renseignement économique sera également examinée dans la présente section, de même que celle des entreprises de gardiennage, de sécurité et des services internes de gardiennage.

A. L'influence et le lobbying.

Jean-Louis Levet considère que les pratiques d'influence constituent l'une des quatre fonctions essentielles de l'intelligence économique ([37]).

L'Etat et les pouvoirs publics deviennent en effet une cible importante sur le marché du renseignement. A tous les niveaux (européen, fédéral, régional, communautaire, provincial ou communal), le pouvoir politique fait l'objet d'interventions grandissantes, non seulement de la part de gouvernements étrangers, mais aussi de la part de secteurs industriels et professionnels privés qui, de groupes d'intérêt, se transforment en groupes de pression. Ces pressions relèvent pour une large part du lobbying que d'aucun décrivent comme *« l'art d'accommoder l'intérêt général aux intérêts particuliers, économiques ou associatifs. »* Cette pratique occupe des milliers de personnes ou lobbyistes au sein d'entreprises, de fédérations professionnelles ou de cabinets privés.

[37] ean-Louis Levet, *L'intelligence économique, fondements méthodologiques d'une nouvelle démarche, Revue d'intelligence économique*, mars 1997, N° 1, pages 50 / 64.

Le lobbyiste est donc avant tout un courtier en information. Il doit bien connaître les processus politiques et sociaux, les procédures d'élaboration des décisions ainsi que les divers intervenants et leurs intérêts. Il doit pour cela connaître et fréquenter tous les intervenants et alliés possibles dans le jeu compliqué des systèmes d'influence : décideurs politiques, hauts fonctionnaires, syndicats, partis politiques, fédérations patronales, chambres de commerce, associations, groupes de pression, etc. A cet effet, il s'efforce de se rendre sympathique et cultivant ses relations personnelles et en rendant des services autour de lui.

L'influence auprès des décideurs politiques ne peut s'exercer sans une vaste culture générale, juridique et technique et sans une mémoire des très nombreux textes en gestation. Le lobbyiste performant ne se contente pas de suivre les événements, il anticipe les menaces ou les opportunités, par exemple en prévoyant les marchés publics qui se dessinent, en intervenant directement auprès des cabinets ministériels concernés pour proposer des modifications de texte au stade des projets de lois et de décrets, en informant les politiciens sur les conséquences de certaines propositions, etc.

Bruxelles, siège des institutions de l'Union européenne, compte plusieurs centaines de groupes d'intérêts pratiquant un lobbying quotidien. Ces professionnels de l'influence observent, analysent et conseillent les entreprises désireuses d'infléchir la position des administrations préparant les futures normes industrielles, environnementales ou commerciales ; celles-ci sont en effet l'objet de négociations acharnées entre intérêts contradictoires.

Comme l'intelligence économique, le lobbying se pratique aussi bien au sein qu'à l'extérieur de l'entreprise. Les possibilités d'influence et de lobbying des entreprises étant plus limitées que celles de l'Etat, il arrive donc que celles-ci s'adressent à des organismes officiels, à des ministères ou à des organismes internationaux pour défendre leurs intérêts, notamment au niveau de l'élaboration des normes. Le Japon et les Etats-Unis s'en sont faits d'ailleurs une spécialité.

Mais il existe aussi des fédérations patronales ou professionnelles pour veiller aux intérêts de leurs secteurs auprès de ces diverses autorités politiques. Elles se donnent pour mission de développer l'image de l'industrie qu'elles défendent par le biais de campagnes d'information ou de sensibilisation et elles utilisent à cet effet des stratégies claires et pro-actives qui précisent les objectifs à atteindre à court, moyen et long termes. Elles développent aussi des partenariats stratégiques avec d'autres organisations patronales.

Ces organisations jouent un rôle de premier plan dans l'élaboration des normes de protection de l'environnement, et dans toutes les matières qui concernent l'octroi des permis d'exploiter, les taxes environnementales (la taxe CO^2), les écotaxes, l'épuration des eaux, le traitement et la valorisation des déchets, les rejets atmosphériques, les plans de prévention des emballages, le bruit, etc. Un des enjeux actuellement importants du lobbysme se dessine avec le projet de certaines ONG d'élaborer un standard ISO pour la moralité des entreprises (« *corporate social responsibility* »).

Dans les marchés publics les plus importants, il existe aussi un lobbying tout aussi actif que celui agissant au niveau européen. Aux niveaux national et international, les grands contrats, notamment en matière d'armement et d'équipements militaires, n'échappent pas aux pressions des lobbyistes qui tentent de convaincre les plus hautes autorités. Par ailleurs, certains gouvernements n'hésitent pas à recourir eux-aussi à des lobbyistes privés pour défendre leurs intérêts devant des instances internationales, auprès d'Etats étrangers ou pour élaborer leur stratégie de communication dans des situation de crises internationales ([38] - [39]).

A force de se manifester, les groupes de pression ont mis au point des démarches diverses pour obtenir avant les autres les précieuses informations, des techniques d'expression et de communication pour faire passer leur message et, parfois, pour prendre l'opinion à témoin ([40]). Des ouvrages s'écrivent et se vendent destinés à enseigner les techniques d'influence ([41]). Pour un prix d'environ 900 € par jour, des instituts privés de formation organisent des séminaires destinés à former des cadres d'entreprises dans cette discipline ([42]).

Un rapport du commissaire européen de la Justice et des Affaires intérieures, daté du 2 juin 2003 et intitulé « *une politique globale de l'Union européenne* » indique que des « *affaires ont montré qu'il pouvait exister des liens secrets (triangulaires entre les titulaires de fonctions publiques, le monde des affaires et des représentants des partenaires sociaux et d'autres groupes d'intérêt se situant à l'interface entre le secteur public et le secteur privé. Très souvent, des donations non déclarées sont faites au mépris des obligations légales, pour influencer des décisions politiques ou économiques importantes* ». Ce rapport devrait initier un prochain débat au Parlement européen sur les pratiques du lobbying et sur la manière de les réglementer.

B. La négociation de contrats internationaux - les intermédiaires.

De formations professionnelles diverses, les intermédiaires ont pour spécialité d'intervenir sur les marchés internationaux en vue d'obtenir des contrats pour le compte d'entreprises et d'en retirer ainsi le paiement de commissions. On trouve beaucoup d'intermédiaires sur le marché de l'armement, mais également dans d'autres domaines civils. Ils agissent le plus souvent dans la conclusion de contrats avec des pays du Tiers monde et, à présent avec des pays d'Europe de l'Est.

---

[38] Ainsi, le gouvernement argentin aurait chargé un cabinet privé de convaincre le Congrès américain de soutenir les finances de Buenos Aires (IOL n° 428 du 25 avril 2002).

[39] C'est aussi une firme privée de lobbying qui a été chargée d'élaborer la stratégie de communication du département de la défense américain pour justifier le recours à la force militaire en Irak (IOL n°441du 21/11/2002)

[40] Les débats à propos de la réglementation de la vente et de la publicité du tabac en ont été, pendant des années, une illustration.

[41] « *Le lobbying et ses secrets » guide des techniques d'influence,* Michel Clamen – Dunod, Paris 2000, 3e édition

[42] Voir par exemple le « *Development Institute International* » à Paris sur le site Internet www.development-institute.com

Classés à part dans le monde du renseignement économique, les intermédiaires sont des personnages discrets ou hauts en couleurs qui n'exercent pas vraiment un métier reconnu comme tel dans les milieux économiques. Patients et prudents, solitaires, avec ou sans structures, ils s'appliquent à tisser des réseaux et à cultiver leurs relations avec le monde politique et les décideurs au plus haut niveau. La force d'un bon intermédiaire réside dans sa capacité de relier à haut niveau le monde politique et le monde économique. Cette force repose sur la confiance qu'il s'applique à inspirer à des interlocuteurs de cultures différentes. Celle-ci exige beaucoup plus que de pures compétences techniques et commerciales. En marge de négociations officielles, l'intermédiaire efficace est capable de débloquer une situation par sa connaissance des enjeux sous-jacents qui ne sont pas toujours financiers mais qui peuvent relever du « diplomatique » ou du « protocolaire ». A cet effet, le bon intermédiaire cultive sa culture générale et sa bonne connaissance des mécanismes décisionnels des milieux qu'il vise et dont la logique échappe quelquefois à la pensée cartésienne des industriels occidentaux.

Les commissions réclamées varient de 3% à 10 %, mais certains intermédiaires s'estimant incontournables pour certains contrats demandent davantage. Le paiement de commissions fait, à présent, partie du processus normal de négociation d'importants contrats internationaux, mais cette pratique n'est pas sans poser une série de problèmes éthiques. Dans certaines affaires, cela s'apparente à des cas de corruption.

Il se dit que les intermédiaires excellent dans les pays ayant une faible culture en matière de renseignement et qui ne pratiquent que des approches commerciales classiques. Cette situation étant celle de la Belgique, nul ne s'étonnera de trouver chez nous bon nombre d'intermédiaires. En France, certains intermédiaires ont vu leur rôle officialisé par l'Etat ou par certaines sociétés mixtes.

Quelques-unes des pratiques développées par certains intermédiaires pourraient toutefois être bientôt visées par une nouvelle incrimination pénale résultant de la prochaine mise en application de la convention pénale de Strasbourg sur la corruption. Cette convention enjoint en effet aux parties d'adopter les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale le trafic d'influence. Le gouvernement belge a toutefois proposé d'émettre une réserve à cette obligation afin d'exclure de son champ d'application le trafic d'influence privé ([43]).

C. La guerre et la contre-guerre de l'information – Info War.

Une des techniques les plus agressives mise en œuvre à des fins de lobbying et d'influence est la guerre de l'information ou « l'Info War » ([44]). Il s'agit, pour une nation ou pour un secteur industriel, de défendre ses industries en diffusant un flot d'informations et/ou de désinformations déstabilisatrices envers les concurrents. Cette pratique peut également être utilisée comme nouvelle forme d'activisme par des groupes de pression ou par des ONG qui ont bien compris que le talon d'Achille des entreprises était leur image de marque.

---

43 Sénat de Belgique, session extraordinaire du 9 octobre 2003 – 3 – 230/1 : projet de loi portant assentiment à la Convention pénale sur la corruption, faite à Strasbourg le 27 janvier 1999.

44 Philippe Baumard et Christian Harbulot, *Perspectives historiques de l'Intelligence économique, Revue d'intelligence économique*, Mars 1997, N° 1, pages 50/64

De véritables campagnes de dénigrement peuvent parfois être mises en œuvre sur le réseau Internet et dans les médias pour attenter à la réputation d'un Etat, d'un secteur d'industrie ou d'activités, d'un concurrent, etc.. Jean-Louis Levet décrit ainsi cette pratique d'influence : *« La guerre de l'information est l'utilisation offensive de l'information afin d'affaiblir, de déstabiliser, ou détruire un adversaire* ([45]). Les techniques utilisées peuvent être de la désinformation, de la manipulation d'information, des rumeurs et de la propagande.

Il existe donc des sociétés qui offrent sur le marché des services et programmes informatiques destinés à suivre en temps réel l'image d'une entreprise et à anticiper les atteintes qui pourraient lui être portées à la suite d'accidents industriels, d'affaires judiciaires ou de campagnes de dénigrement.

Toute prévention et contre-guerre de l'information suppose la connaissance et la maîtrise des techniques offensives de la guerre de l'information. Dans ce contexte, quelques fabricants de solutions de veille sur Internet configurent leurs programmes pour analyser en continu la teneur de l'information relative à une marque ou à des produits. La finesse des observations qu'on retire de quelques indicateurs stratégiques (volume de citations d'une marque, nombres de citations critiques, évolution des associations négatives et des sujets sensibles, etc.) permet de mesurer mondialement la montée en puissance des sujets à risque et d'identifier les auteurs de campagnes de dénigrement. Ces firmes effectuent des passages dans les "*news groups*" et sur certains sites Web afin de surveiller, étudier et analyser tous les forums et conversations entre internautes pour le compte de ses clients. Grâce à des logiciels de recherche très puissants, ces agences peuvent analyser l'ensemble des lieux de conversation virtuels pour y dénicher des mots ou des expressions-clés. Cette masse de données est traitée par des scientifiques, sociologues, sémiologues qui en font une analyse ciblée selon la demande du client. Des entreprises étatiques peuvent aussi recourir à ces services particuliers ([46]).

Ce type de recherche permet l'intervention plus précoce de cabinets de lobbying chargés de contrer toute atteinte à la réputation d'une entreprise ou d'un pays.

D. L'expertise comptable et l'audit de management.

Il convient d'examiner ici les services offerts par les cabinets d'audit et de consultance. Quelques grands cabinets anglo-saxons se partagent principalement ce marché de la consultance et des audits d'entreprises. Selon les époques ceux-ci ont sont appelés les *Big Six,* les *Big Five* et maintenant les *Big Four* dans la littérature spécialisée. En effet, ces cabinets sont en constante évolution ; ils s'associent, se démantèlent ou disparaissent à l'occasion d'importantes opérations financières ou de faillites. L'audit lui-même est une discipline en mouvement. Les tous premiers mandats des auditeurs comportaient surtout des missions d'inspections des comptes d'entreprises. Par la suite, l'accent fut davantage mis sur la consultance et l'audit de fraude. En tant que consultant, l'auditeur examine si les moyens mis en œuvre au sein d'une organisation lui permettent d'atteindre les objectifs fixés. En tant qu'auditeur de fraude, il examine et propose des systèmes de contrôle internes pour éviter que des fraudes se produisent ou pour les découvrir le plus vite possible. Dans ce cadre, il arrive de plus en plus fréquemment que des auditeurs privés collaborent avec des magistrats et des services de police.

---

[45] Jean-Louis Levet, *L'intelligence économique, fondements méthodologiques d'une nouvelle démarche, Revue d'intelligence économique*, mars 1997, N° 1, pages 35/49.

[46] On cite ici le cas d'un groupe pétrochimique proche du roi d'Arabie Saoudite qui emploie une firme privée britannique afin de suivre et de contrer les campagnes menées par des ONG de défense des droits de l'homme (*Amnesty International* en particulier) susceptibles de critiquer l'Arabie Saoudite IOL n° 428 du 28 avril au 15 mai 2002.

Initialement composés de réviseurs d'entreprises, d'économistes et de juristes, les départements d'audits se sont progressivement ouverts à de nouvelles problématiques (informatique, environnement, etc.) et ils se retrouvent à présent composés d'équipes multidisciplinaires. Mais pour affiner encore leurs produits, quelques cabinets se sont aussi investis dans le secteur de l'intelligence économique (voir plus loin).

Organisés en réseaux internationaux et disposant de moyens financiers et humains impressionnants, ces géants de la consultance pénètrent donc au cœur des grandes entreprises pour vérifier leurs comptes, mais aussi pour réaliser des audits de toutes natures (comptable, informatique, juridique, fiscal et technique), disséquer leurs faiblesses, donner des conseils stratégiques, piloter des fusions, des rachats, etc. Les banques anglaises et américaines exigent souvent la signature de l'un de ces cabinets d'audit pour authentifier les bilans des entreprises étrangères qui désirent s'implanter aux Etats-Unis ou en Grande-Bretagne. Ces grands réseaux anglo-saxons n'ont pas d'équivalents dans les autres pays européens où ils occupent une position de force. Ces cabinets concentrent donc ainsi chez eux une quantité impressionnante d'informations sur des sociétés cotées en Bourse. A plusieurs reprises, la presse économique européenne s'est émue de cet impressionnant « droit de regard » sur des entreprises.

Une conséquence de ces récentes faillites d'entreprises américaines comme *Enron* ou *WorldCom* a été de provoquer une crise de confiance dans l'information financière sur les entreprises américaines. Ceci a incité les banques à procéder à des vérifications de *due intelligence* sur les résultats financiers de leurs principaux clients. Le secteur du renseignement privé s'adapte à cette nouvelle demande, d'où l'apparition de nouveaux cabinets dédiés à l'investigation financière. Aux Etats-Unis, ce secteur d'activités est à présent placé sous le contrôle de l'administration via le *Public Accounting Oversight Board.*

E. Le gardiennage de sécurité.

La problématique des entreprises de gardiennage, de sécurité et des services internes de gardiennage, ne devrait pas être abordée dans le présent rapport puisqu'en Belgique, la loi du 10 avril 1990 réglementant l'activité des entreprises de gardiennage ou de sécurité ainsi que les services internes de gardiennage interdit explicitement à ces entreprises d'exercer des activités de renseignement privé. Cette loi fixe aussi les conditions dans lesquelles ces entreprises doivent être agréées par le ministre de l'Intérieur et leur interdit d'exercer tout autre activé que la surveillance et la protection de biens mobiliers, de valeurs et d'immeubles, la protection de personnes, la gestion de centraux d'alarme, ainsi que la surveillance et le contrôle de personnes dans le cadre du maintien de la sécurité dans des lieux accessibles au public. Il est explicitement interdit à ces entreprises de s'immiscer ou d'intervenir dans des conflits politique ou de travail, d'intervenir lors de ou à l'occasion d'activités syndicales ou à finalité politique. Il leur est également interdit *« d'exercer une surveillance sur les opinions politiques, philosophiques, religieuses ou syndicales (ou sur l'appartenance mutualiste), ainsi que sur l'expression de ces opinions (ou de cette appartenance) et de créer à cette fin des banques de données ».* Ces entreprises ne peuvent non plus « *communiquer à des tiers une information quelconque sur leurs clients et les membres du personnel de ces derniers* ».

Enfin, la loi du 19 juillet 1991 organisant la profession de détective privé interdit à ces personnes d'exercer simultanément une autre activité dans une entreprise de gardiennage, de sécurité ou dans un service interne de gardiennage.

Néanmoins, le Comité permanent R pense que des zones d'ombres existent sur l'utilisation qui peut être faite des renseignements auxquels les firmes de gardiennage accèdent dans l'exercice de leur activité. Impliquées de près dans la mise en œuvre des mesures de sécurité des entreprises et dans la surveillance électronique des allées et venues des membres de leurs personnels, ces firmes de gardiennage accumulent en effet un impressionnant stock de données sur leurs clients.

Le contrôle administratif de l'application de la loi du 10 avril 1990 est confié au SPF « Politique de sécurité et de prévention » service qui dépend du Ministre de l'Intérieur. Le ministre de l'Intérieur doit faire annuellement rapport par écrit à la Chambre des représentants.

L'article 6 bis de la loi du 10 avril 1990 prévoit que la Sûreté de l'Etat peut être chargée de mener des enquêtes sur les conditions de moralité auxquelles les responsables et les collaborateurs de ces entreprises doivent satisfaire pour être agréées. Néanmoins, à ce jour, la Sûreté de l'Etat n'a encore jamais été chargée de procéder à ce type d'enquête.

Un projet de loi adopté en mars 2004([47]) vise notamment à accélérer la procédure d'autorisation en prévoyant la possibilité de demander directement l'avis de la Sûreté de l'État et du procureur du Roi du lieu où l'entreprise de gardiennage a son siège d'exploitation. Ce n'est que lorsque l'entreprise concernée n'a pas de siège d'exploitation en Belgique que l'avis du ministre de la Justice doit être demandé ; celui-ci demandera ensuite à son tour l'avis de la Sûreté de l'État et du Collège des procureurs généraux.

3.2.9. L'apparition de nouveaux champs d'activités du renseignement privé : le renseignement « humanitaire » et le renseignement « militant ».

Selon les experts du Comité R, il est très probable que l'on assistera, dans les années à venir à la naissance et au développement d'un renseignement « humanitaire » que se partageront le secteur privé et certaines ONG. L'instabilité du monde et la multiplication des « *low intensity conflicts* » et des situations de grande détresse qui en résulteront justifieront peut-être la naissance de cette nouvelle discipline.

Eric Denécé, directeur du Centre d'Etude et de Prospective Stratégique (CEPS) à Paris, pense quant à lui qu'on pourrait voir bientôt apparaître des structures humanitaires plus ou moins factices chargées de couvrir des activités de recueil de renseignements pour le compte d'autres structures (entreprises, services officiels) ([48]).

Par ailleurs, les conflits et drames vécus par la Somalie, l'ex-Yougoslavie (de la Croatie au Kosovo) ou le Rwanda au cours des dix dernières années ont prouvé à suffisance que les services de renseignement d'Etat n'étaient guère préparés pour cette tâche. Plutôt tournés vers la pénétration des structures étatiques, ces services n'ont, en général, qu'une piètre connaissance des réalités du « pays profond » et ils peinent manifestement à discerner et à analyser les « signaux faibles », c'est-à-dire les signes avant-coureurs de conflits pouvant déboucher sur un génocide ou une catastrophe humanitaire.

---

47 Chambre, 5e session période 2002/2003 15 2328/003 DOC 50

48 Les nouvelles pratiques agressives de la compétition économique – Conférence donnée le 12 février 2003 au Club d'Intelligence Economique (IAE) de Paris.

Depuis les années nonante, de plus en plus d'organisations issues de la société civile ont aussi vu le jour pour s'impliquer dans des actions ayant pour objet de promouvoir au niveau international les droits de l'homme, l'aide humanitaire, la santé, le respect de l'environnement, le développement des populations du Tiers-monde, l'équité du commerce mondial, etc. Bien que non reconnues par le droit international, certaines ONG sont pourtant devenues des lobbies très influents et ont ainsi acquis un statut de partenaire privilégié à l'égard de certaines organisations internationales (Nations Unies, Organisation Mondiale de la Santé, Commission européenne, Conseil de l'Europe, etc.) ou de certains Etats.

Tandis que certaines ONG organisent des manifestations à l'occasion de rencontres politiques internationales, d'autres mènent des enquêtes et publient des rapports dénonçant des situations contraires aux principes qu'elles défendent, comme par exemple des violations des droits de l'homme commises par les autorités de certains Etats, des trafics d'armes, des collusions d'intérêts financiers et politiques contraires à une exploitation et à une répartition raisonnable de certaines ressources naturelles (pétrole, commerce du bois exotique, de diamants, etc.).

A cette fin, certaines ONG disposent d'importants réseaux de relations tissées auprès d'organisations internationales et dans des lieux de pouvoir ; elles utilisent également des techniques d'enquêtes et des méthodes de recueil de renseignements dignes de véritables services de renseignement.

3.2.10. Le renseignement militaire privé.

Les experts du Comité constatent que la fin de la guerre froide et l'effondrement du bloc soviétique ont eu deux conséquences qui ont radicalement modifié le paysage du mercenariat.

Les conflits locaux se sont multipliés et ont nécessité l'implication de personnels militaires bien formés et aptes à encadrer les troupes locales. A l'Ouest, mais aussi à l'Est, de nombreux militaires ont été démobilisés, licenciés ou mis en retraite alors qu'ils étaient encore jeunes et aptes à combattre. Ceux-ci ont naturellement eu tendance à vendre leurs services dans ces guerres qui éclataient un peu partout.

Un troisième élément a renforcé cette évolution : la tendance à la privatisation de la guerre (comme du renseignement) venant essentiellement du monde anglo-saxon. Cette tendance s'explique selon les experts par trois facteurs :

- Le premier, économique, est la tendance naturelle du marché à aussi s'étendre à des fonctions qui étaient, dans le passé, celles des Etats.
- Le deuxième, également économique, est que le recours au secteur privé permet souvent aux Etats de gérer leurs interventions à meilleur coût (« cost effective way »), même dans le domaine militaire.
- Le troisième, d'ordre stratégique, est que l'intervention d'acteurs privés bien formés et fiables permet aux Etats de continuer à défendre leurs intérêts et leur influence tout en offrant, si nécessaire, la possibilité d'user du « plausible denial »[49].

[49] Voir point 3.5.5.

C'est ainsi qu'à la faveur de l'ultra libéralisme ambiant et de l'émergence de nouveaux types de conflits dits « de basse intensité », on a vu apparaître principalement aux Etats-Unis et en Grande Bretagne, mais aussi en Afrique du Sud, des firmes spécialisées dans les services de défense. Celles-ci portent de nombreuses appellations comme « *Sociétés Militaires Privées » (SMP), « Private Military Companies » (PMCs*) ou plus simplement « *Sociétés de sécurité »* ou encore *« Private Security Firms »* offrant sur le marché bien plus que des services de mercenaires. Le présent rapport utilisera l'expression « *Sociétés Militaires Privées » (SMP).*

Constituées par des anciens officiers supérieurs et/ou par d'anciens agents de renseignement, ces firmes commerciales se spécialisent dans l'exécution de missions d'audit, de formation et d'assistance dans des domaines purement militaires pour compte de certains gouvernements.

Contrairement aux firmes de renseignement commercial, la trace des SMP est extrêmement difficile à suivre. La plupart d'entre elles fuient la publicité et n'ont, par exemple, aucune politique de communication ni d'utilisation de sites sur l'Internet ; les experts désignés par le Comité permanent l'ont constaté dans leurs recherches. Leurs clients savent où les trouver et connaissent leurs compétences.

L'éventail des activités qu'elles proposent est en effet très large : conseils en matière de politique intérieure, internationale, de défense et de sécurité (évaluation de menaces, identification d'enjeux), aide à la définition de procédures et de plans stratégiques pour les ministères de la Défense, enquêtes de sécurité, recrutement et formation d'officiers, de sous-officiers et entraînement de troupes armées, fourniture ou location de matériel militaire ou de télécommunication avec formation à son utilisation, fourniture de gardes du corps et de personnel de surveillance, acheminement de matériel militaire et de troupes sur des terrains d'opérations, déminage, inspections de sécurité, soutien logistique et accompagnement de missions humanitaires et de maintien de la paix, etc.

Selon David Isenberg, un expert en matière de défense, rares seraient ces sociétés qui impliqueraient directement leur personnel dans des activités de combat à proprement parler ([50]). Il est vrai qu'une convention adoptée en 1989 par l'ONU mais entrée en vigueur seulement en 2001, faute de ratifications suffisantes jusqu'à cette date, tend à réprimer l'utilisation, le financement et l'instruction des mercenaires. Est considérée comme mercenaire *« toute personne recrutée dans le pays ou à l'étranger pour combattre dans un conflit armé »* et cela pour une rémunération *« nettement supérieure »* à celle que reçoivent les soldats du pays concerné.

Mais pour beaucoup d'observateurs, il ne fait aucun doute que ces Sociétés Militaires Privées pratiquent aussi la collecte de renseignements militaires pour le compte de leurs clients.

Ces SMP affirment bien sûr qu'elles n'entreprennent jamais d'opérations « *contre les intérêts nationaux des gouvernements occidentaux* » mais leurs affaires sont souvent secrètes et elles obéissent surtout à la logique économique du secteur privé.

Elles interviennent partout dans le monde et notamment dans des pays représentant des enjeux géopolitiques et géo-économiques importants mais où les Etats, les organisations internationales, les ONGs ou encore les grandes entreprises multinationales ne veulent ou ne peuvent s'engager en tant que tels.

---

[50] David Isenberg : « *Regulated Private Military Firms have a role*", Defense News, 11 – 17 March 2002, page 13.

Des SMP sont aussi de plus en plus souvent louées par des Etats du Tiers Monde bénéficiant de ressources suffisantes mais dépourvus d'instruments militaires de qualité. De même, et ceci est assez nouveau, des sociétés privées ont recours aux SMP pour protéger leurs installations et activités dans des zones sensibles. Il en va de même pour de grosses ONG et des médias de taille.

Selon les experts du Comité, il existe des « signaux faibles » auxquels les services de renseignement peuvent être attentifs pour prévoir l'intervention imminente d'une SMP sur une zone d'intervention. Le plus pertinent de ces signaux faibles est, selon eux, l'accroissement du trafic aérien impliquant de petites compagnies privées. Ceci peut signifier un acheminement important de troupes et de matériel qui ne peut se faire par les grandes lignes aériennes étatiques ou commerciales.

Aux Etats-Unis le secteur des SMP est soumis, comme le commerce des armes, à une seule et même législation, *the International Traffic in Arms Regulations (ITAR)*. Le Parlement britannique a récemment examiné une proposition de loi tendant à soumettre ce secteur d'activités à une législation spécifique et à un contrôle du gouvernement. Selon Jack Straw, ministre britannique des Affaires étrangères, nous nous trouvons dans un monde où les guerres sont à petite échelle et où les Etats sont faibles. Nombre de ces Etats ont besoin d'aide extérieure pour maintenir l'ordre chez eux. Il se peut aussi que la communauté internationale ressente le besoin d'intervenir davantage. Dans le même temps, dans les pays développés, le secteur privé est en train de s'impliquer de plus en plus dans des activités militaires et de sécurité. Dès lors que certains Etats ne sont pas ou ne sont plus en mesure d'exercer leurs prérogatives régaliennes, l'ONU pourrait être amenée à se tourner vers d'autres acteurs pour agir ([51]). C'est ainsi que le projet de réglementation du gouvernement britannique voit volontiers les SMP jouer un rôle actif dans les opérations de maintien de la paix et humanitaires, dans le domaine de la logistique, du déminage, du gardiennage et même des négociations lors de prises d'otages, ceci, tant pour le compte de gouvernements que d'ONGs et d'entreprises multinationales. C'est ce que le gouvernement britannique appelle l'*outsourcing* (l'externalisation) des tâches de sécurité ([52]). Il semble que de hauts responsables politiques et militaires français aient aussi le projet de créer un cadre juridique permettant le développement en France de SMP ([53]).

Bien sûr, tout ceci soulève différentes questions de fonds quant à la souveraineté nationale, la responsabilités de ces SMP devant les instances nationales et internationales et le respect des droits de l'Homme.

3.3. Les professionnels du renseignement privé et de l'intelligence économique.

Parmi les prestataires de services en matière de renseignement et d'intelligence économique, on relève différents types d'acteurs émanant de milieux professionnels divers et porteurs aussi de diverses qualifications professionnelles. Parmi eux, on trouve notamment :

---

51 Les experts du Comité relèvent ainsi qu'un consortium de firmes privées, dénommé « *International Peace Operations Association* », s'est créé aux Etats-Unis dans le but de faire du lobbying auprès des Nations Unies et de leur proposer les services des sociétés qu'il regroupe (notamment MPRI) dans des opérations de maintien de la paix (http://www.ipoaonline.org/)

52 FCO, Private Military Companies – Options for Regulation, Green Paper by the Foreign Secretary, Jack Straw, HC 577, 10 February 2002.

53 Intelligence on line n°456 du 3 juillet 2003.

- des détectives privés,
- des documentalistes;
- des ingénieurs et des techniciens;
- des spécialistes du marketing et des ingénieurs commerciaux ;
- des anciens policiers, militaires et agents des services de renseignement de l'Etat ;
- des informaticiens.

Ces prestations peuvent aussi impliquer des journalistes, des reporters, des juristes, des comptables et des réviseurs d'entreprises auxquels il faut maintenant ajouter les titulaires de ces nouveaux diplômes spécialisés en intelligence économique. Bref, de nombreuses professions et disciplines peuvent être concernées de près ou de loin par le renseignement privé d'ordre économique.

3.3.1. Les détectives privés ([54]).

A. Généralités.

Le cas des détectives privés doit être traité de manière distincte. Les recherches effectuées par des détectives privés se situent à la fois sur le terrain des enquêtes privées de police destinées à rassembler les preuves d'une infraction et celui du recueil de renseignements.

En France, un détective privé est appelé « *agent de recherches privées* ». Le détective privé entre dans le cycle de l'information à partir du moment où l'information ouverte ne suffit plus.

Il n'existe pas, à ce jour, de statistiques fiables sur le pourcentage exact d'enquêtes réalisées par les détectives privés dans le secteur des affaires. On sait pourtant que des firmes de renseignement privés utilisent régulièrement les services de détectives privés à qui elles sous traitent certaines missions.

Les experts du Comité permanent R constatent en effet que depuis quelques années, un certain nombre de détectives présentent, notamment sur leur site, de nouvelles compétences fortement liées à l'air du temps. En clair, ils affirment être capables de mener des actions de contre-espionnage économique, de lutte contre la fraude en entreprises, des enquêtes sur les salariés ou les candidats à l'embauche. Historiquement, les détectives privés se sont lancés très tôt dans la protection industrielle et le renseignement économique.

Selon diverses sources d'informations en Belgique, les contrats pour compte d'entreprises représenteraient entre 80 et 90 % du chiffre d'affaires des détectives privés. Il s'agirait de missions d'enquêtes de moralité portant sur des candidats à l'embauche, de recherches en matière de contre-façons, de concurrence déloyale, de fraudes, d'escroqueries, de corruption, etc. [55].

D'autres sources avancent que sur les quelque 900 détectives privés agréés en Belgique, 700 à 750 travailleraient pour le compte de compagnies d'assurance, soit en qualité de salarié, soit comme indépendant. Leurs principales missions consisteraient dans la détection d'escroqueries à l'assurance. ([56]). Dans les faits, les experts du Comité permanents R estiment que, seuls, une poignée de ces bureaux de détectives sont en mesure d'effectuer des missions relevant réellement du renseignement économique.

---

54 Voir Christophe Deloire, Histoire secrète des détectives privés, éditions J.C. Lattès, Paris, 2001.
55 F. Moser et M. Borry, *«Intelligence stratégique et espionnage économique»* - Luc Pire 2001
56 'Le Soir' du 14 mai 2002

B. Définition légale de la profession de détective privé. (57)

En Belgique, la loi du 19 juillet 1991 organise et encadre de manière très stricte la profession de détective privé. La définition légale des activités permises aux détectives privés situe leurs missions aussi bien dans le domaine de la police privée que dans celui du renseignement privé.

Au sens de la loi, est considérée comme détective privé *toute personne physique qui, dans un lien de subordination ou non, exerce habituellement contre rémunération et pour le compte d'autrui des activités* déterminées. Ce n'est que dans l'éventualité où toutes ces caractéristiques sont réunies dans le chef d'une seule et même personne, que nous avons affaire à un détective et que la loi trouve à s'appliquer.

Une "*personne physique"* : seules des personnes physiques peuvent porter le titre de détective privé (ou sont désignées de cette façon par le législateur). Contrairement à la réglementation relative au secteur du gardiennage, il est donc exclu que des personnes morales relèvent du champ d'application de la loi. Par conséquent, seuls des particuliers ont le droit (habituellement et contre rémunération) d'effectuer des recherches; l'entreprise (ou un service d'une entreprise) en tant que telle ne peut le faire.

Les activités que peuvent exercer les détectives privés sont les suivantes :

1. "*Rechercher des personnes disparues ou des biens perdus ou volés*". Cette activité de police n'est pas l'objet du présent rapport.

2. "*Recueillir des informations relatives à l'état civil, à la conduite, à la moralité et à la solvabilité de personnes »*. Bien que ce ne soit pas explicite, le législateur entendait apparemment par « personnes » qui font l'objet de ces recherches, aussi bien les personnes physiques que les personnes morales[58]. Cela signifie que le recueil d'informations sur la solvabilité d'entreprises peut constituer une activité de détective. Ainsi, les personnes qui travaillent dans des entreprises d'informations commerciales peuvent relever du champ d'application de la loi organisant la profession de détective privé.

3. *"Réunir des éléments de preuve ou constater des faits qui donnent ou peuvent donner lieu à des conflits entre personnes ou qui peuvent être utilisés pour mettre fin à ces conflits".* Ici encore, l'on entend par "personnes" aussi bien des personnes physiques que les personnes morales.

---

57 Voir J. Cappelle et W. Van Laethem, *"Le statut du détective privé"*, Bruxelles, Politeia, 1998, II-10 e.s.

58 Doc. Parl, Sénat, 1990/1991 - Avis du Conseil d'Etat 1259/1, p. 35. On pourrait déduire de l'énumération des notions "d'état civil", de "conduite" et de "moralité" à l'article 1, § 1, 2° de la loi, que le législateur n'a visé que les personnes physiques. Si au début de l'article 1er de la loi, la notion de "personnes physiques" ne vise que les détectives comme des particuliers, la notion dans le reste de l'article 1er, cette notion vise aussi bien les personnes physiques que les personnes morales

4. «*Rechercher des activités d'espionnage industriel"* : Le législateur n'a pas précisé ce qu'il faut entendre par « espionnage industriel ». Selon la rare littérature belge spécialisée dans de domaine, l'on pourrait définir cette activité comme la collecte secrète de données par une entreprise dans le but d'avoir une idée aussi complète que possible des potentialités et des intentions du concurrent, pour pouvoir déterminer ainsi sa propre politique[59]. La Sûreté de l'Etat parle d'espionnage économique et concurrentiel selon que l'acte est posé par un organisme public ou une organisation privée. Dans ces définitions, l'accent est davantage placé sur le caractère illégal de l'activité.

5. «*Exercer toute autre activité définie par un arrêté royal délibéré en Conseil des ministres* ». Bien qu'il ne fût pas dans l'intention immédiate du législateur de réglementer d'autres activités que celles énumérées du 1 à 4, une ouverture a été laissée pour l'avenir. La demande en évolution rapide sur ce marché de services peut, en effet, faire en sorte que cela devienne nécessaire plus tard. Cette disposition offre la possibilité de placer certaines activités jugées problématiques dans le champ d'application (et donc des mécanismes de contrôle) de cette loi.

6. *« Habituellement »* : les activités précitées doivent être exercées « habituellement ». Celui qui pratique occasionnellement des activités de renseignement (économique) n'est pas contrôlé.

7. *« Pour le compte d'autrui »* : le donneur d'ordre peut être en même temps, dans certains cas, l'employeur du détective. C'est souvent le cas pour les personnes qui travaillent dans le secteur de l'assurance comme inspecteur de fraudes. En matière d'*intelligence économique*, on recourra aussi souvent à l'expertise « maison ».

8. « *Dans un lien de subordination ou non »* : la personne qui mène habituellement des activités de détective contre rémunération pour le compte d'autrui, relève de l'application de la loi. A ce moment là, peu importe que le détective travaille sous statut d'indépendant ou de salarié. Il est donc parfaitement possible qu'un détective privé soit occupé dans une entreprise dans les liens d'un contrat de travail.

9. « *Contre rémunération »* : le champ d'application de la loi est enfin délimité par l'exigence de la rémunération. La personne qui mène des activités de recherche sans rémunération n'est pas soumise à la loi.

Il ne sera donc pas toujours aussi facile de déterminer qui tombe dans le champ d'application de la loi organisant la profession de détective privé. La qualification adéquate dépend, en effet, entièrement de la méthode de travail concrète d'une personne et est tout à fait indépendante du titre qu'elle porte ou de la structure de l'entreprise ou du service dans lequel elle fonctionne. C'est ainsi que des personnes travaillant dans des entreprises privées qui mènent des activités de renseignement économique sont susceptibles d'être considérées comme détectives et d'autres pas.

C. L'accès à la profession de détective privé et les conditions d'exercice.

En Belgique, nul ne peut exercer la profession de détective privé ou se faire connaître comme tel s'il n'a pas préalablement obtenu à cette fin l'autorisation du Ministre de l'Intérieur, après avis du Ministre de la Justice.

---

[59] *"Kwetsbare kennis. Over bedrijfseconomische spionage en informatiebeveiliging"* - B. Hoogenboom et M.Cools. Alphen aan de Rijn, Samson, 1996 - p. 139

Un projet de loi modifiant la loi sur les détectives privés prévoit explicitement que l'avis de la Sûreté de l'État devra aussi être sollicité. L'agréation d'un détective privé est attestée par une carte d'identification dont il doit être porteur et qui bientôt contiendra une carte à puce infalsifiable.

Parmi les conditions fixées pour obtenir cette autorisation (nationalité, âge, domiciliation, moralité, formation professionnelle), figurent aussi celle de ne pas exercer simultanément d'activités dans une entreprise de gardiennage, de sécurité ou dans un service interne de gardiennage et celle de ne pas avoir été, au cours des cinq dernières années, membre d'un service de police ou d'un service de renseignement soumis au contrôle des Comités permanents P et R. Ce délai est porté à dix ans pour celui qui a été révoqué ou démis d'office d'un tel emploi.
S'il a fait autrefois partie d'un service de police ou d'un service public de renseignement, le détective privé ne peut en faire état dans l'exercice de ses activités professionnelles. Il ne peut aucunement se présenter comme membre d'un tel service. Un détective privé ne peut d'ailleurs exercer ses activités au profit d'une personne de droit public, sauf accord du Ministre de l'Intérieur.

Anticipant la loi du 30 juin 1994 *"relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées***"**, la loi du 19 juillet 1991 interdisait déjà strictement au détective privé de recourir à ces méthodes à l'insu des personnes dans des lieux non accessibles au public ([60]).

Il est également interdit au détective privé « *d'espionner ou de faire espionner ou de prendre ou de faire prendre intentionnellement des vues de personnes qui se trouvent dans des lieux non accessibles au public, à l'aide d'un appareil quelconque, sans que le gestionnaire du lieu et les personnes concernées aient donné leur consentement à cette fin* » (article 5). Il lui est interdit de recueillir sur des personnes « *des informations relatives à leurs convictions politiques, religieuses, philosophiques ou syndicales et à l'expression de ces convictions (ou relatives à leur appartenance mutualiste)* ». Il lui est également interdit de recueillir des « *informations relatives au penchant sexuel* » de personnes, « *sauf s'il s'agit d'un comportement contraire à la loi ou qui peut constituer un motif de divorce* » à la requête d'un des conjoints. Le détective privé ne peut non plus recueillir de l'information sur la santé, sur les « *origines sociales ou ethniques* » des personnes (article 7).

Comme pour les entreprises et services de gardiennage, le contrôle administratif de l'application de la loi du 19 juillet 1991 est confié à la Direction générale de la Police Générale du Royaume, service qui dépend du Ministre de l'Intérieur. Les fonctionnaires de la PGR sont investis de larges pouvoirs d'investigation afin d'être en mesure de vérifier la bonne application de la loi. Le ministre de l'Intérieur doit pourtant faire annuellement rapport par écrit à la Chambre des représentants.

[60] A ce propos, on soulignera pourtant que, si l'utilisation de matériels d'écoute et d'interception est interdite en Belgique, la fabrication, la vente ou la possession de tels dispositifs n'y fait encore l'objet d'aucune réglementation. Il est par ailleurs très facile de se procurer ce type de matériel dans plusieurs pays voisins où ces dispositifs sont en vente libre ou via certains sites Internet

D. Les entreprises et détectives étrangers ([61])

Les ressortissants d'un Etat membre de l'Union européenne

Le détective qui est ressortissant d'un Etat membre de la CE et qui n'a aucun établissement en Belgique, mais qui veut malgré tout y mener certaines activités de recherche, doit (tout comme le détective belge qui n'a pas d'établissement chez nous) tenir compte de règles très spécifiques.

Le fait que ces détectives soient déjà soumis à l'une ou l'autre réglementation dans leur pays d'origine, ne fait aucune différence. Ils doivent également obtenir une autorisation pour exercer des activités de détective dans notre pays.

Le législateur ne fait, à cet égard, aucune distinction entre activités durables ou temporaires. Il peut ainsi arriver qu'un détective non établi en Belgique traite une mission qui lui a été confiée dans son agence étrangère.

L'évolution de l'affaire le conduit toutefois à devoir se rendre sur le territoire belge pour y effectuer une activité de recherche déterminée. Ce détective privé devra obtenir à l'avance une autorisation de la part des pouvoirs publics belges.

Les conditions d'autorisation auxquelles ces détectives sont soumis, sont similaires à celles des détectives établis en Belgique. Pour ces détectives, le législateur fixe toutefois une condition supplémentaire importante : ils doivent élire un lieu d'établissement ~~(certes fictifs)~~ chez un(e) détective/personne de contact en Belgique.

La raison en est claire. Ces détectives pourraient, à défaut de lieu d'établissement en Belgique, échapper à tout contrôle. Pour éviter cet écueil, ils doivent au moins disposer dans notre pays d'un point de contact obligatoire.

La personne de contact doit se porter garante du respect par le détective « étranger » des règles relatives à la surveillance des citoyens et à l'interdiction de recueillir certaines informations liées à la vie privée. Cette personne de contact du détective « *exerce (…) le contrôle nécessaire au respect de ses obligations »*.

On vise son obligation de se porter garant que son collègue respecte les interdictions précitées. Cela semble tout sauf évident. Cette obligation ne peut être, en effet, respectée que si la personne de contact suit son « hôte » (ou même ses « hôtes ») à la trace dans ses activités, ce qui est totalement impraticable.

On a opté pour cette solution parce que l'État belge ne peut lui-même exercer aucun contrôle sur un détective privé établi à l'étranger. Le contrôle du détective établi en Belgique implique que ce dernier est responsable vis-à-vis des instances belges de contrôle. Il ne peut se soustraire à ses obligations. Dans le cas contraire, il risque une suspension, voire un retrait de sa propre autorisation.

Une double « obligation de signalement » incombe à la personne de contact. Tout d'abord, il fait rapport chaque trimestre au ministre de l'Intérieur sur la manière dont le détective privé, pour lequel il se porte garant, exerce ses activités. De plus, la personne de contact est tenue, dès qu'elle en a connaissance, d'informer les autorités compétentes de tout manquement du détective privé dont il se porte garant.

---

[61] Voir J. Cappelle et W. Van Laethem, *"Le statut du détective privé"*, Bruxelles, Politeia, 1998, II-10 e.s.

Les non-ressortissants d'un État membre de l'Union européenne

Les personnes qui relèvent de la qualification de « détective privé », mais qui ne sont pas des ressortissants de l'Union européenne, ne peuvent exercer en aucune manière des activités de détective en Belgique, même si cette activité est simplement sporadique. Le législateur motive cette option radicale parce que le contrôle des conditions en matière de moralité, d'incompatibilités ou d'interdiction de passage de la frontière, ne peut certainement pas toujours être fait en confiance dans des Etats non-membres de la l'Union européenne.

La manière dont la loi organisant la profession de détective privé est interprétée, permet en principe d'exercer un contrôle sur la majeure partie des « activités de renseignement économique » qui sont énumérées dans la littérature spécialisée.

3.3.2. Les bibliothécaires - documentalistes.

Dans bien des entreprises encore, le centre de documentation représente encore l'unique service dédié à l'information ou à la veille technologique.

Les documentalistes formeraient donc le vivier numériquement le plus important des professionnels en intelligence économique. Il s'agit de bibliothécaires – documentalistes qui ont développé une autre conception de leur profession que celle de simples « conservateurs » de documents. Ouverts aux besoins de leurs employeurs, ils cherchent à donner une valeur ajoutée à leurs recherches documentaires et ils s'impliquent dans les dispositifs de veille technologique. Ils sont au cœur des demandes d'informations de leur entreprise et ils disposent donc d'une vue privilégiée sur ses besoins en la matière. Ils disposent aussi d'une parfaite maîtrise des outils documentaires : ils gèrent les abonnements, connaissent les techniques de classement et d'archivage, ils savent questionner les banques de données, exploiter le réseau Internet, constituer des thésaurus, etc.

3.3.3. Les ingénieurs et les techniciens.

Des ingénieurs ou des techniciens de formation s'orientent volontiers vers la veille technologique, non pas en fonction de leurs connaissances des techniques de l'information, mais plutôt grâce aux connaissances approfondies du domaine industriel ou scientifique qu'ils ont acquises et qu'ils mettent en œuvre dans leurs entreprises. Spécialistes de la consultation des brevets industriels, ces veilleurs « spontanés » savent ce qui est important ou non pour le développement de leur entreprise. Ce sont eux qui sont chargés de trouver, de traiter, de diffuser et de conserver l'information relative à l'évolution technologique du secteur d'activité qui les emploie.

3.3.4. Les économistes et les ingénieurs commerciaux.

Les économistes, les ingénieurs commerciaux ou les spécialistes de la finance s'orientent plutôt vers la veille concurrentielle et stratégique. Ils occupent aussi une place importante dans les services d'analyse des services de renseignement privés.

3.3.5. Les anciens policiers, militaires et agents des services de renseignement de l'Etat.

Aux Etats-Unis, en Grande Bretagne et en France, ils sont nombreux les anciens fonctionnaires de police qui apportent leur connaissance des techniques d'enquêtes au service des enquêtes privées et du renseignement économique. Militaires retraités et anciens agents des services de renseignement sont aussi de plus en plus nombreux à se reconvertir dans l'intelligence économique, particulièrement aux Etats-Unis où le gouvernement les a en effet encouragé à se reconvertir dans le secteur privé après la fin de la guerre froide.

Le phénomène se développe aussi en France où l'on a d'abord trouvé d'anciens militaires engagés comme responsables de la protection et du gardiennage. On voit à présent d'anciens membres de la DST ou de la DGSE apparaître dans le domaine de la sécurité informatique ou du renseignement économique. Leur domaine d'intervention privilégié est bien sûr tout ce qui touche aux marchés de l'armement.
Dans le sens inverse, il est aussi intéressant de noter la récente nomination d'un ancien dirigeant d'entreprises à la tête de la Direction du renseignement de la DGSE ([62]). Ce rapprochement entre militaires, agents de renseignement et monde économique se traduit par une meilleure prise en compte du concept de guerre économique par les entreprises. Leur esprit « *security minded* » ou *« intelligence minded »*, leur sens de l'autorité, leur connaissance des techniques de collecte de renseignements, leur expérience et les relations qu'ils conservent dans leur ancien milieu professionnel en font des collaborateurs très appréciés malgré leur manque de connaissance du monde des entreprises privées. Mais leur image d'ancien agent secret dissuade encore certains employeurs de recourir à leurs services.

Il faut noter que la législation française interdit aux fonctionnaires de la police nationale, aux officiers et sous-officiers de la gendarmerie nationale ou de l'armée d'exercer une activité de recherche privée durant les cinq années suivant la date à laquelle ils ont cessé définitivement ou temporairement leurs fonctions, sans avoir obtenu au préalable l'autorisation écrite, selon le cas, du ministre de l'Intérieur ou du ministre de la Défense nationale. Par ailleurs, il leur est interdit de faire état de leur qualité d'ancien fonctionnaire de police ou d'ancien militaire dans l'exercice de leur activité de recherche privée ([63]).

3.4. L'enseignement et la formation au renseignement économique.

Depuis quelques années déjà, plusieurs universités et hautes écoles françaises se sont attachées à intégrer l'intelligence économique dans leurs programmes de cours et de formation, souvent avec l'aide ou même à l'instigation d'anciens militaires et de responsables de la sécurité nationale. Des établissements d'enseignement privés forment le personnel des entreprises. Ces institutions délivrent des diplômes d'enseignement de troisième cycle, des « diplômes d'enseignement supérieur spécialisé (DESS) » ou des « mastères spécialisés en intelligence économique », en « veille stratégique ou concurrentielle », en « management des systèmes d'information et d'organisation », en « information et sécurité », etc. L'annuaire européen des professionnels de l'Intelligence économique mentionne 25 universités et autres établissements d'enseignement proposant ce genre de formation en France.

---

62 IOL n° 440 du 7 au 20 novembre 2002.

63 Articles 21 et 27 de la loi n° 83-629 du 12 juillet 1983 réglementant des activités privées de sécurité, créé par la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure (http://www.legifrance.gouv.fr/).

Selon le rapport du député français Bernard Carayon « *Intelligence économique, compétitivité et cohésion sociale* » ([64]), cet enseignement universitaire, trop théorique, trop généraliste et dispensé sans doctrine ni contrôle est inadapté aux besoins des entreprises. Le député rapporteur développe dès lors une série de propositions afin de mettre cet enseignement au service d'une politique nationale et de l'adapter aux besoins réels des entreprises.

Dans les pays anglo-saxons, la « *business intelligence* » ou « *corporate intelligence* » fait partie du programme d'enseignement des *MBA* « *Master of Business Administration*).

3.5. Les méthodes des professionnels du renseignement privé

Pratique ancienne donc, voire très ancienne, le renseignement privé commence pourtant seulement à sortir des pratiques empiriques pour être théorisé. Il en résulte que les méthodes utilisées sont encore entourées du plus grand flou. Face à l'espionnage économique ou de concurrence, dont ils se déclarent les adversaires déterminés, les promoteurs du renseignement et de l'intelligence économique prétendent ne mettre en œuvre que des procédés licites et légaux, c'est-à-dire essentiellement la consultation de sources ouvertes. Certains reconnaissent toutefois qu'ils utilisent à l'occasion des méthodes du renseignement militaire, comme par exemple le recours à des images satellitaires. Selon les experts du Comité R, les méthodes d'observation ou de récolte du renseignement pratiquées par les sociétés de renseignement privé ne diffèrent guère de celles des services de renseignement d'Etat.([65]).

En fait, les méthodes de recherche utilisées varieront selon qu'elles visent à capter ce qu'il est convenu d'appeler de l'information « blanche » (c-à-d de sources ouvertes), de l'information « grise » (informelle) ou de l'information « noire » (c-à-d couverte par le secret).

3.5.1. La collecte de renseignements à partir de sources ouvertes (open sources).

L'information « blanche » comprend tout ce qui est disponible, gratuitement ou moyennant paiement, dans les sources accessibles au public : journaux, revues, magazines, études, bilans, brevets, publications officielles, banques de données, etc., le tout pouvant à présent se retrouver sur des sites Internet.

Ainsi par exemple, si le brevet entraîne le monopole d'exploitation d'un procédé ou d'une invention au profit de son inventeur mais il ne garantit aucunement sa confidentialité. Bien au contraire, la documentation contenue dans les brevets rendus publics constitue une source ouverte extrêmement riche de renseignements. En outre, les statistiques de brevets constituent une sources de signaux faibles annonciateurs de l'émergence de nouvelles technologies. C'est d'ailleurs la raison pour laquelle certaines entreprises hésitent à déposer des brevets pour certaines de leurs inventions dont elles désirent garder le secret.

L'utilisation de logiciels spécialisés dans la collecte, l'analyse et la gestion de ces données est donc devenue courante dans le renseignement privé. Les experts en donnent l'aperçu suivant ([66]).

---

64 Voir le point 5.2.3. plus loin.

65 Voir à ce sujet Comité permanent R, rapport d'activités de l'année 2000 (pages 124 à 127) (NL 130 – 133)

66 Pour mieux connaître ces utilitaires, on peut consulter les sites web www.veille.com ou www.agentland.fr.

A. Les outils de collecte d'information.

Les moteurs de recherche : il s'agit de programmes puissants capables de rechercher sur les sites Web ou dans les groupes de discussion toutes les pages comportant un mot ou une expression donnée. Ces outils donnent accès à l'information la plus pointue sur les sites Web accessibles au public ([67]), et même sur ceux qui ne le sont pas. Ainsi, le Web caché ou *deep Web* ([68]) serait plus de cinq cent fois plus étendu que le World Wide Web connu (il contiendrait une capacité d'informations de 7.500 terabytes comparée aux dix neuf terabytes du Web commun). Des firmes privées se spécialisent donc dans l'utilisation de ces outils informatiques et de techniques qui ont été conçus à l'origine pour l'usage des services de police ou de renseignement.

Outre les moteurs de recherche classiques, certains moteurs se distinguent aujourd'hui comme « agents d'alerte » dans le cadre d'une veille, c'est-à-dire d'une surveillance systématique de l'environnement informationnel. Ils sont généralement gratuits ou peu onéreux ([69]).

Les méta-moteurs : ce sont des programmes informatiques puissants qui permettent de rechercher des adresses ou des sites sur plusieurs moteurs en parallèle en triant les résultats et en éliminant les doublons. ([70]).

Les aspirateurs de sites : ce genre d'utilitaire permet de charger le contenu d'un site, partiellement ou totalement, sur un disque dur. Ce procédé offre comme avantages de ne pas se faire repérer par des visites fréquentes sur un même site, de pouvoir analyser son contenu de manière globale (*text mining*), et de pouvoir identifier les modifications apportées entre les différentes versions du même site ([71]).

B. Les outils de gestion et d'analyse de l'information.

« Query & reporting, data warehouse, data mining » : il s'agit de programmes dits de ***« Business Intelligence »*** qui permettent aux entreprises de traiter et d'analyser d'importantes quantités de données chiffrées (chiffres de vente, exportation, indicateurs financiers) afin d'en tirer une vue globale et des enseignements prospectifs ([72]).

Bibliométrie, infométrie et scientométrie : une nouvelle tendance de logiciels d'information et lexicaux sont issus de laboratoires universitaires de recherche. Travaillant sur les fréquences d'apparitions de certains mots, ils permettent notamment de trouver la littérature la plus pertinente dans certains domaines choisis, de surveiller la parution d'ouvrages et d'articles, le dépôt de brevets et de les insérer dans un système automatique de veille.

---

67 Exemples : *Google, Alltheweb, Sybion, DejaNews*

68 Pour des moteurs sur cette partie du web, on peut consulter http://urfist.univ-lyon1.fr ou www.invisibleweb.com

69 Exemples : Netmind, Bulleyes, ou ***Kartoo*** (France), un moteur de recherche cartographique disponible gratuitement sur Internet.

70 Le plus utilisé est ***Copernic*** dont la version professionnelle contient une fonction « veille » clairement paramétrée. Autre exemple : ***Dogfile***

71 Quelques exemples : ***MemoWeb, Teleport Pro***.

72 Exemples : ***Cognos, SAS, SPSS*** (Etats-Unis) et ***Business Objects*** (France) sont les programmes les plus cités et présents dans les grandes entreprises. Ces programmes sont assez onéreux. Voir aussi ***Enterprise Miner*** et ***Intelligent Miner (IBM).***

L'analyse systématique des résumés d'articles scientifiques dans des domaines donnés permet ainsi de voir apparaître de nouveaux concepts scientifiques ou des tendances émergentes assimilées à des « signaux faibles », de connaître les principaux chercheurs scientifiques travaillant dans un domaine de pointe particulier, d'identifier de nouveaux noms et de mettre ainsi à jour les réseaux formels et informels de collaborations, etc.

Il existe ainsi des **outils de cartographie de l'information** permettant de visualiser des domaines de recherche en quelques heures (exemples Kartoo (www.kartoo.com) ou WordMapper (http://www.activeille.net/carto/wordmapper.htm).

Les programmes de « text-mining » permettent de procéder à une analyse sémantique et/ou linguistique de textes ou de données ([73]).

Parmi ces logiciels standards, on en trouve ayant reçu un paramétrage spécifique, voire un développement sur mesure, en fonction de l'environnement spécifique d'une entreprise et de sa stratégie en matière de renseignement. On se trouve alors en présence de véritables logiciels d'intelligence économique.

C. Développement et perspectives.

Les experts du Comité estiment que l'utilisation en Belgique de ces programmes spécialisés est encore limitée à quelques grandes entreprises ou associations professionnelles. Ceci est dû aux prix relativement élevés (50 à 100 000 € en moyenne) pour une application complète et opérationnelle (c'est-à-dire incluant les fonctionnalités de collecte, analyse et gestion) d'une part et à la nécessité de disposer de compétences particulières (compétence en gestion de l'information stratégique, cartographie des connaissances,…) pour en tirer profit d'autre part. Néanmoins les experts estiment que la morosité dans le secteur informatique, l'évolution des logiciels et l'émergence de la discipline "intelligence stratégique" devraient favoriser l'utilisation de ces programmes dans de moyennes entreprises dans un premier temps, par des PME ou des sociétés de service et de conseil dans un second. Parmi les outils cités, les applications de "text mining" seraient promises à un bel avenir de par leur capacité à isoler et identifier des signaux faibles dans une masse d'information. Selon les experts, il s'agira là d'un défi que les entreprises belges devraient apprendre à relever dans le contexte d'une compétitivité croissante.

Le Comité nuance toutefois cet avis des experts en observant que certains logiciels de linguistique ([74]) détournés de leur usage premier, peuvent déjà être utilisés avec des résultats probants dans des applications de « text mining » et de bibliométrie. On peut s'attendre à ce que certains programmes quittent le domaine universitaire pour entrer dans la panoplie des outils du veilleur.

Dans son rapport « *Technology Forecast 2003 - 2005*» ([75]), la firme américaine *PricewaterhouseCoopers* prédit que les programmes informatiques de *business intelligence* figureront parmi les principales innovations technologiques dont les entreprises en quête de performances s'équiperont dans les prochains mois.

---

[73] Exemples : ***Tropes Zoom V6*** un moteur de recherche sémantique de la société *Acetic* (France), Leximine, U-Map.

[74] Comme ***WordSmith Tools*** par exemple.

[75] Disponible sur http://www.pwcglobal.com

3.5.2. Quand passe-t-on du renseignement économique à l'espionnage économique ?

Dans bien des esprits, les notions de renseignement et d'espionnage sont confondues. En réalité, on peut collecter du renseignement de bien des manières sans jamais recourir à l'espionnage ni commettre d'acte illégal. Face au flou qui caractérise certaines de leurs pratiques, les professionnels du renseignement économique proclament volontiers leur souci de respecter la légalité et une certaine déontologie. Mais pour que cette affirmation ait un sens, il faudrait une définition claire de l'espionnage économique ou industriel, de ce que l'on peut faire et de ce que l'on ne doit pas faire. Or la barrière entre ce qui est permis et ce qui est interdit est loin d'être lisible en toutes circonstances. Les débats en cours parmi les professionnels révèlent les désaccords sur la nature des pratiques qui peuvent être considérées comme acceptables ou non ([76]).

La législation belge ignore le **secret des affaires** et ne connaît pas de définition de **l'espionnage économique ou industriel,** ce qui est une grave lacune pour la protection des entreprises. Celles-ci sont en effet dépositaires d'un nombre considérable d'informations dont l'addition représente un véritable patrimoine à protéger.

Aux Etats-Unis, **l'espionnage économique** est défini comme « *the unlawful or clandestine targeting or acquisition of sensitive financial, trade, or economic policy information, proprietary economic information or critical technologies* ». C'est donc le caractère illégal ou clandestin de la recherche d'informations qui caractérise l'espionnage économique dans cette définition qui en exclut par conséquent le recueil d'informations disponibles dans le domaine public.

Le Service Canadien du Renseignement de Sécurité estime par contre que l'espionnage économique est le fait pour un gouvernement d'utiliser ou de faciliter l'utilisation de moyens illégaux, clandestins, coercitifs ou trompeurs pour avoir accès sans autorisation à des renseignements économiques ou technologiques en propriété exclusive, afin d'en retirer des avantages économiques ([77]).

Aux Etats-Unis, **l'espionnage industriel** est défini comme « *the activity conducted by a foreign government of by a foreign company with the direct assistance of a foreign government against a private US company for the sole purpose of acquiring commercial secrets* ».

Pour le Service Canadien du Renseignement de Sécurité, l'espionnage industriel est le fait, pour un organisme du secteur privé ou ses représentants, d'utiliser ou de faciliter l'utilisation de moyens illégaux, clandestins, coercitifs ou trompeurs pour avoir accès sans autorisation à des renseignements économiques ou technologiques en propriété exclusive, afin d'en retirer des avantages économiques ([78]).

Dans une note du 31 mai 2001, la Sûreté de l'Etat propose de retenir les définitions du Service Canadien du Renseignement de Sécurité tout en préférant l'expression « **espionnage de concurrence** » à celle d'espionnage industriel.

---

[76] Jérôme Dupré, *Renseignement et entreprises,* Lavauzelle, 2002 – section III pages 70 et suivantes.

[77] "Série d'aperçus" n° 6 - mai 1998, publication du Service canadien de Renseignement de Sécurité.

[78] "Série d'aperçus" n° 6 - mai 1998, publication du Service canadien de Renseignement de Sécurité.

Dans ce document interne soumis à l'approbation du Comité ministériel du renseignement et de la sécurité, la Sûreté de l'Etat écrit : "*Si le mandant de l'espion est de nationalité belge, il s'agit d'espionnage industriel et ce domaine n'est pas du ressort de la sûreté de l'Etat. Si par contre, le mandant est originaire d'un pays étranger, il s'agit d'espionnage économique et la lutte contre cette activité s'inscrit parfaitement dans le cadre des missions de la Sûreté de l'Etat."* Pour ce service, ce serait donc la nationalité du mandant de l'espion qui ferait la différence entre l'espionnage économique et l'espionnage industriel.

Le Comité permanent R émet de nettes réserves sur cette vue des choses qui, ne prenant en compte que l'origine nationale ou étrangère de la menace, néglige l'intérêt même (scientifique ou économique) menacé. Par ailleurs, comment attribuer d'emblée une nationalité au mandant d'un espion, et déterminer ainsi la compétence de la Sûreté de l'Etat, alors que les restructurations industrielles et la globalisation des procédés au niveau mondial rendent difficile l'attribution d'une nationalité aux entreprises ?

En fin de compte, l'espionnage viserait à capter de l'information « noire », c à d celle qui est protégée et que l'on ne trouve pas dans le domaine public parce que le propriétaire a pris des mesures pour la garder secrète ou confidentielle. Il s'agit généralement d'informations relatives à des transactions commerciales, à des activités et ressources économiques, à des projets de recherche et développement, à des secrets de fabrication, à des inventions qui n'ont pas été déposées comme brevets, à des technologies de pointes, etc. Ce sont ces informations que le droit américain protège comme « *trade secrets* » ou « *proprietary information* » ([79]).

Face à l'espionnage économique ou de concurrence, dont ils se déclarent les adversaires déterminés, les promoteurs du renseignement et de l'intelligence économique déclarent généralement qu'ils ne mettent en œuvre que des procédés licites et légaux, c'est-à-dire essentiellement la consultation de sources ouvertes. L'argument le plus souvent véhiculé pour conforter cette assertion consiste à affirmer que la moindre transgression de la loi nuirait considérablement à la réputation de la société et écornerait son image de marque. Cet argument est recevable dans une certaine mesure. Il est évidemment impossible d'affirmer que telle ou telle entreprise ne respecte pas la légalité tant qu'elle n'a pas été prise sur le fait ou encouru une condamnation. La fréquentation de séminaires consacrés à ce sujet permet pourtant d'entendre évoquées à mots couverts d'autres pratiques situées en « zone grise », c'est-à-dire à la marge de l'éthique, sinon de la légalité.

Selon les experts du Comité R, *« il est possible d'effectuer une distinction entre les sociétés de renseignement privées qui pratiquent la recherche d'informations de type industriel ou économique de manière légale des autres, notamment par le type de services qu'elles offrent et leur façon de travailler. Une société qui effectue des recherches uniquement sur Internet, même avec des outils extrêmement performants, sera moins « suspecte » de tomber dans l'illégalité. En revanche, toute société proposant des services de due intelligence ou qui affirme réaliser des recherches de terrain ou faire du renseignement offensif, pourrait être davantage suspectée d'officier à tout le moins en « zone grise », c'est-à-dire aux limites de la légalité.* »

Les ouvrages et les séminaires consacrés au renseignement économique recommandent aux entreprises de veiller attentivement à la nature et au contenu des contrats qu'elles signent avec les professionnels de ce secteur. L'aspect déontologique doit être mentionné dans ces contrats et ne pas se limiter à une clause de style. Dans cette démarche, le problème de la confidentialité se pose notamment pour les projets de recherche.

[79] *The Economic Espionage Act EEA of 1996*

Mais à cet égard, les sous-traitants du renseignement économique font aussi valoir qu'ils sont davantage tenu par une obligation de moyens à mettre en œuvre, que de résultats à obtenir. Dans le contexte de concurrence acharnée auquel ils sont confrontés, les sous-traitants du renseignement se plient plutôt aux exigences des entreprises clientes en matière de moyens d'investigation (légaux ou non) et de confidentialité, qui peuvent varier selon les demandes, et aller jusqu'à des contrats d'exclusivité. La mise en œuvre de règles de déontologie dépendrait donc surtout de l'entreprise cliente.

Les experts du Comité R, sont plus affirmatifs. A les en croire, les acteurs du monde du renseignement privé ne se contentent pas seulement de pratiquer du « renseignement défensif » en n'utilisant que des méthodes légales. Pour eux, la réalité est quelque peu différente :

« Certes, certains cabinets d'intelligence économique prétendant jouer un rôle dans le renseignement privé se bornent, par exemple, à entretenir des veilles sur Internet. On est ici, bien évidemment, dans le domaine de la légalité la plus pure. Mais le « rendement » de cette activité en termes d'acquisition de renseignement est, par la force des choses, relativement limité. La veille (autrement dit l'acquisition de renseignements de sources ouvertes, même difficilement accessibles) est effectivement une partie du travail de renseignement mais elle ne peut prétendre constituer « tout le renseignement »: de tous temps, les professionnels ont su que le renseignement « ouvert » constitue, suivant les cas, de 80 à 95% du matériel nécessaire à la connaissance préalable à laquelle concourt l'espionnage. Mais ces 80 à 95% ne servent pas à grand chose si les 5% à 20% de renseignement « fermé » manquent. Or, pour acquérir ce renseignement de sources fermées (documents internes d'entreprises, protocoles et résultats de recherche et développement, stratégies commerciales et moyens mis en place etc.) il faudra, presque obligatoirement, à un moment où l'autre, « franchir la ligne.

Certes, le fait de travailler sur « sources fermées » n'est pas, en soi, illégal. Aucune loi interdit à un individu ou à une société de prendre contact avec le détenteur de « renseignement fermé » et de le faire parler, pour autant que cela se passe ouvertement, sans corruption, sans contrainte et sans subterfuge. Mais même dans ce cas, le délit ne sera pas loin car, tôt ou tard, l'opérateur se retrouvera en possession d'informations commerciales ou industrielles qui ne lui sont pas destinées et pourra donc être accusé de recel de vol (ou de détournement) d'informations privilégiées. De plus, soyons clair : le cas idyllique décrit ci-dessus qui verrait le détenteur d'informations confidentielles les livrer presque de lui-même relève quasiment de l'hypothèse d'école. Dans la réalité, pour acquérir ce renseignement fermé, l'opérateur devra accumuler les délits, des « moins graves » (usurpation d'identité ou de fonction) aux plus lourds : organisation de surveillances physiques pouvant être assimilées à une intrusion dans la vie privée, corruption, chantage, vol, interception de courrier, écoutes illégales, intrusion informatique etc.

Ce sombre tableau explique clairement pourquoi aucun opérateur sérieux et ayant pignon sur rue n'admettra jamais qu'il se livre au renseignement « offensif ». Pourtant, sans jouer les naïfs, on peut se demander à quoi servent, si personne ne pratique cette collecte offensive, ces sociétés et cabinets « défensifs » qui fleurissent dans de nombreuses capitales depuis quelques années. La réalité est moins rose. Oui, le renseignement privé offensif existe. Oui, il est pratiqué régulièrement. Les auteurs de ce rapport ont eu, ainsi, connaissance de cas sur lesquels ils ne peuvent s'étendre où, à l'étranger, des bureaux de sociétés commerciales ont été « visités » de nuit par des équipes de « casseurs » protégés de surcroît par des policiers chargés d'éloigner les éventuels curieux » ([80]).

[80] Rapport d'expertise « *le renseignement privé en Belgique* » adressé au Comité R en février 2003.

Ce commentaire que les experts portent sur le monde du renseignement privé semble être confirmé par les autorités américaines. Chaque année, le président des Etats-Unis présente un rapport au Congrès sur l'ensemble des menaces que l'espionnage économique et/ou industriel fait peser contre l'industrie américaine. Ce rapport est préparé par *l'Office of the National Counterintelligence Executive* avec la collaboration des services de renseignement officiels. Selon le rapport présenté en 2001, 60 % des activités suspectes de recueil d'informations relatives à l'industrie de défense US sont menées par des firmes commerciales étrangères ou par des individus sans rapport avec des gouvernements étrangers. Le rapport considère que ces activités de recueil de renseignements, bien que menées légalement et de manière tout à fait ouverte, peuvent être dommageables pour l'économie américaine. *« These collection efforts often serve as precursors to economic espionage ».*

En France aussi, on le verra plus loin, la Direction de la surveillance du territoire (DST) est attentive au phénomène « d'atomisation » et de « privatisation » de la menace qui, selon elle, rend difficile à la fois son identification et sa neutralisation.

3.5.3. Quelques méthodes de recueil de l'information « grise».

L'information « grise » est celle qui, n'étant pas publiée, s'obtient de manière informelle, auprès de personnes appartenant à l'entreprise elle-même ou du monde extérieur (clients, fournisseurs, sous-traitants, experts, etc.). Ces informations, pas nécessairement confidentielles, peuvent être riches d'une grande valeur ajoutée et contenir des « signaux faibles » annonceurs de menaces ou d'opportunités pour l'organisation.

La littérature relative à l'intelligence économique ou aux services de renseignement livre de nombreuses manières de recueillir ce type d'information, des plus classiques aux plus sophistiquées, mais pas nécessairement déloyales ou illicites. En voici ici quelque aperçu.

- Les réseaux d'informateurs des entreprises.

Certaines entreprises mettent sur pied de véritables réseaux de correspondants spécialisés chargés d'observer et de recueillir des renseignements de nature informelle, non structurée. Ils utilisent, pour transmettre leurs informations aux analystes, des formulaires standardisés aussi appelés "capteurs d'informations". Ce sont soit des "voyageurs" de l'entreprise, soit des représentants, qui par leurs contacts privilégiés avec les fournisseurs, les sous-traitants, les clients, peuvent obtenir de l'information fraîche sur les besoins, les projets, les évolutions des concurrents.

- La fréquentation des expositions, des colloques, congrès, foires et salons.

Ces rassemblements d'experts constituent une source considérable d'information pour les professionnels de l'intelligence économique, ... et pour les espions. Les comptes rendus en sont systématiquement étudiés. Les prospectus intéressants sont récoltés pour être passés au scanner et introduits dans des banques de données. Des échantillons sont analysés, des pièces sont photographiées - parfois clandestinement -, des spécimens sont acquis (ou dérobés) pour être décortiqués. Les questions débattues en séances contiennent des informations très intéressantes, les conversations de couloirs, autour d'un "drink", également.

3.5.4. Quelques méthodes de recueil de l'information «noire».

Les méthodes les plus classiques et brutales sont bien sûr le vol de documents, la fouille des poubelles, la subornation de personnes, la corruption, le chantage, les menaces, etc. Des techniques de manipulation peuvent également être mises en oeuvre, sans parler des technologies nouvelles. On peut aussi citer les méthodes suivantes.

- La surveillance des scientifiques en voyage à l'étranger.

Un rapport présenté le 25 juin 2000 par le *"General accounting Office"* (GAO) au Congrès des Etats-Unis a recensé 75 tentatives récentes d'espionnage à l'étranger sur des savants nucléaires américains. Ce rapport, basé sur le compte-rendu de centaines de voyages effectués par des scientifiques de par le monde expose des cas de mises sous écoute dans des hôtels, de fouilles d'effets personnels ou bien encore d'offres de services de prostituées. Le GAO recommande que les voyages de certains scientifiques à l'étranger soient soumis à l'autorisation préalable des services de contre-espionnage.

- Les chercheurs universitaires en stage à l'étranger.

Les laboratoires universitaires peuvent aussi être la cible de services de renseignement. La technique consiste à y envoyer des étudiants boursiers ou des chercheurs stagiaires pour y recueillir des informations importantes d'ordre scientifique. Le séjour terminé, l'étudiant chercheur rentre dans son pays d'origine où il sera soigneusement "débriefé" de ses connaissances techniques et scientifiques fraîchement acquises. Le monde académique se montre en général assez ouvert à la diffusion du savoir et à la coopération internationale, d'où la facilité pour n'importe quel chercheur de recueillir des informations sans même les avoir demandées. C'est la raison pour laquelle les services de sécurité devraient être attentifs à la présence de stagiaires étrangers dans des laboratoires de recherches de pointe.

- La prise de participation dans une société.

Certaines entreprises engagées dans la veille technologique dispose de fonds d'investissement afin de prendre des participations dans des sociétés de haute technologie. Une personne "neutre", agissant pour le compte d'une compagnie (ou d'un Etat) qui désire rester dans l'ombre, procède grâce à des sociétés-écrans et des relais à la prise de participation dans la société cible, par exemple lorsque celle-ci est fournisseur dans un secteur de pointe. Cela permet d'avoir accès à des informations d'ordre technologique, éventuellement à du matériel classifié ou de vendre du matériel soumis à embargo.

- Les faux appels d'offres.

Un Etat fait savoir par des appels d'offres qu'il désire se rendre acquéreur d'une licence d'exploitation ou d'une usine livrée clé sur porte. Aussitôt sollicitées, les grandes sociétés réagissent en dépêchant sur place leurs ingénieurs commerciaux. Les tractations traînant en longueur, les sociétés en lice fournissent de plus en plus d'informations sur leur offre sans y voir malice, espérant obtenir le marché. Elles livrent ainsi des renseignements qu'attendait le pays demandeur. Une firme privée peut aussi agir de la sorte en se présentant, via un cabinet d'investigation, comme client potentiel.

- Les fausses annonces de recrutement.

Les cabinets de recrutement peuvent aussi servir à la collecte de renseignements d'ordre économique. La méthode consiste à publier une annonce alléchante capable de retenir l'attention de cadres ou de chercheurs d'une entreprise cible. Les personnes intéressées par une meilleure proposition salariale, des conditions de recherche améliorées et divers avantages (appartement et voiture de fonction, indemnités diverses, etc.) expédient leur C.V. Celles-ci sont convoquées pour un entretien au cours duquel elles sont longuement interrogées sur leur qualification, leurs travaux antérieurs et actuels. Désireuses d'obtenir le poste, elles sont susceptibles de chercher à se faire valoir en livrant des informations confidentielles qui ne manqueront pas d'intéresser la société concurrente ou l'Etat caché derrière le bureau de recrutement.

- L'interception des communications (COMINT) ([81]).

L'existence d'un réseau global d'interception des communications baptisé "ECHELON" mis en place par les Etats-Unis et par les autres Etats membres de l'alliance UKUSA ([82]) a été médiatisée dés septembre 1998 par une série de rapports destinés au Parlement européen ([83]). Selon le quatrième rapport "*development of surveillance technology and risk of abuse of economic information (an appraisal of technologies for political control) - part 4/4*", ce système orienté à l'origine vers le bloc de l'est, aurait été détourné de sa finalité militaire initiale bien avant l'effondrement des régimes communistes.

Le chapitre 5 intitulé "*Comint and economic intelligence*" contient quelques passages intéressants qui indiquent notamment : *"Comint involving the covert interception of foreign communications has been practiced by almost every advanced nation since international telecommunication became available. Comint is a large-scale industrial activity providing consumers with intelligence on diplomatic, economic and scientific developments.(...) Since the 1960s, following the growth of world trade, the collection of economic intelligence and information about scientific and technical developments has been an increasingly important aspect of Comint".*

La législation des pays membres de l'alliance UKUSA autorise en effet leurs agences de renseignement ainsi que certains ministères à programmer la recherche de renseignements d'ordre économique ou commercial et à en recevoir par le recours au Comint. Ainsi, la loi américaine *Economic Espionage Act* de 1996 permet au FBI et à d'autres agences fédérales de pratiquer des interceptions de communications à des fins de contre espionnage économique. Mais le rapport STOA cite plutôt des cas (sans en apporter la preuve, il est vrai) dans lesquels des firmes européennes auraient été évincées de marchés importants par suite de l'interception de leurs communications au cours de transactions commerciales internationales (*Panavia European Fighter Aircraft consortium, Thomson CSF, Airbus industrie*).

---

81 Le concept Comint (communication intelligence) est défini comme étant la collecte de renseignements effectuée par la surveillance des télécommunications et l'interception de leur contenu.

82 Il s'agirait d'une entente secrète de 1947 organisant la coopération entre les Etats-Unis, le Royaume Uni, le Canada, l'Australie et la Nouvelle Zélande en matière de renseignements.

83 Comité R, rapport d'activités 1999, titre II A. Chapitre 3.

- L'utilisation des nouvelles technologies de la communication.

L'espionnage s'attaque à présent aux techniques modernes de communications électroniques : le piratage des fichiers informatiques, le cyberterrorisme, etc. sont des techniques susceptibles d'être utilisées en vue de saboter les infrastructures d'un Etat ou d'une entreprise. Des spécialistes de l'informatique fouillent en permanence des sites-web d'entreprises concurrentes afin de forcer illégalement les réseaux et de saisir de façon frauduleuse toute une série de données précieuses. Il est également possible de récupérer un ordinateur portable et d'en tirer une copie du disque dur.

3.5.5. La règle des coupe-circuit ou le « Plausible denial » : cloisonnement et moyens financiers importants

Les experts du Comité R décrivent de la manière suivante la règle des « *coupe-circuits* » ou des « *ruptures* » permettant aux services de renseignement privé ou d'Etats de nier l'emploi de méthodes illicites (le « *Plausible denial* »). *Le schéma d'action est le suivant :*

- *La direction d'une entreprise « X » détermine les renseignements qu'elle doit obtenir sur les recherches de son concurrent « Y » ;*
- *La direction de la sécurité ou une cellule plus discrète (éventuellement réduite à un seul individu) est chargée d'organiser la collecte ;*
- *Cet échelon sous-traite la recherche auprès d'une société ou officine spécialisée ;*
- *Cette société spécialisée sous-traite elle-même l'opération auprès d'un ou plusieurs individus dont elle connaît les aptitudes techniques à mener ladite opération.*

Dans ces conditions, le client n'est pas en mesure de connaître la manière dont son fournisseur s'est procuré l'information qu'il a commandée. Ce cloisonnement, avec plusieurs « ruptures » dans la chaîne de commandement et de transmission, assure aussi le commanditaire de la recherche, ses exécutants directs et même la société chargée de cette recherche que, si l'opération tourne mal, on ne pourra en aucun cas remonter jusqu'à eux. Cette manière d'agir n'est qu'un schéma des plus simples. On peut tout à fait imaginer qu'entre l'échelon «3» et l'échelon «4», il y ait encore un ou deux intermédiaires. De même, il est envisageable que, dans le but de « sécuriser » encore davantage l'opération, celle-ci soit menée depuis l'étranger. Ainsi, une société « X » basée en tel pays pourrait avoir recours, pour espionner son concurrent « Y » lui aussi basé dans ce même pays, à une société spécialisée qui passerait par un sous-traitant installé à l'étranger et qui mettrait lui-même en branle une « équipe » originaire d'un autre pays.

Ces pratiques impliquent, à l'évidence, que le renseignement privé offensif requiert tout à la fois de gros moyens financiers (chaque intermédiaire prend sa propre marge et les exécutants doivent être rétribués à hauteur du risque encouru) et la capacité, à un échelon ou l'autre de mobiliser une partie de ces fonds sans laisser de trace comptable ou bancaire. Elles impliquent également, aux échelons d'organisation et d'exécution, l'utilisation de professionnels du renseignement et des opérations spéciales.

On ne peut imaginer en effet que l'exécution de ces « contrats » soit confiée à des truands qui pourraient, par la suite, « tenir » leurs commanditaires. On demande, certes, aux exécutants d'agir illégalement, mais ceux qui les mandatent sont en droit d'en attendre le respect d'une déontologie (pour ne pas parler d'éthique professionnelle…) qui les protégera en cas « d'accident ». C'est ce silence aussi qu'achètent commanditaires et organisateurs . ([84]). »

3.5.6. L'éthique et la déontologie.

Les problèmes éthiques et déontologiques sont l'une des grandes préoccupations des promoteurs de l'intelligence économique. Dans plusieurs pays, des associations professionnelles de l'intelligence économique ont tenté de mettre au point des « codes d'éthique » afin d'établir des conditions d'exercice de la profession et dresser toute une casuistique des questions que l'on peut ou ne peut pas poser à telle ou telle personne dans telle ou telle situation. Ces codes d'éthique sont éminemment contingents et varient selon les latitudes, les longitudes ou les secteurs d'activités. Le principe de base en serait en quelque sorte : « il ne faut pas obtenir une information en dehors de la volonté explicite de celui qui la détient », véritable obligation de ne pas tromper autrui.

Tout comme les services de renseignement étatiques, les firmes privées de renseignement peuvent aussi établir des règles de déontologie tant au niveau de l'engagement du personnel habilité à recueillir le renseignement qu'au niveau des méthodes de recueil du renseignement, du contenu des informations recueillies et de leur utilisation.

Ainsi, certaines firmes déclarent qu'elles refusent d'engager pour exercer l'activité d'agent privé de recherches des personnes qui ont été condamnées ou sanctionnées « pour agissements contraires à l'honneur, à la probité ou aux bonnes mœurs » ou qui ont été déclarées en état de faillite ou de règlement judiciaire.

Dans l'exercice de sa profession, l'enquêteur (l'enquêtrice) peut être tenu par son employeur de respecter certaines règles mises en place dans l'agence, notamment :

- décliner son identité et / ou celle de la société qui l'emploie sur simple demande verbale de son interlocuteur ;
- ne jamais faire passer sa société pour un autre organisme ; sur simple interrogation, il doit en expliciter clairement l'activité ;
- si l'enquête porte sur une personne, faire preuve de la plus grande discrétion afin de ne pas lui porter préjudice, ne rien révéler de défavorable sur elle, vérifier son identité et son adresse pour éviter les homonymies.

Le problème concerne aussi les informations individuelles contenues dans les dossiers personnels ou collectifs. Ces dossiers peuvent concerner aussi bien les membres du personnel de l'entreprise que ses partenaires extérieurs, ses clients, ses fournisseurs, ses consultants, ses banquiers, des journalistes, etc.

Certaines firmes prescrivent notamment qu'un rapport d'enquête ne peut jamais mentionner d'information sans relation avec le dossier (par exemple la race ou l'appartenance politique) ; il ne peut non plus contenir aucun jugement de valeur et doit se limiter d'énumérer des faits

[84] Les commentateurs de la loi belge réglementant la profession de détective privé estiment quant à eux que la relation entre un détective privé et son client est établie *intuitu personae* et que par conséquent un détective privé ne peut sous-traiter une mission à un tiers sans l'accord préalable du commanditaire de cette mission. Voir J. Cappelle en W. Van Laethem, Le statut du détective privé, Brussel, Politeia, 1998, pp.113 et 115).

qui ont été vérifiés. Contenant des données personnelles (état-civil, adresse, numéros de fax et de téléphone, etc.) ces dossiers sont visés par la législation sur la protection de la vie privée et tombent dés lors sous le contrôle de la commission de protection de la vie privée. Certaines firmes mentionnent dans leur charte que l'atteinte à la vie privée d'une personne peut engager leur responsabilité contractuelle, et prescrivent à leur personnel d'avertir un supérieur hiérarchique dès qu'un problème se pose à cet égard. Enfin, les firmes rappellent à leurs agents de recherches que les renseignements qu'ils recueillent sont soumis au secret professionnel. Ceux-ci ne peuvent en faire usage à leur usage personnel ni les divulguer à des tiers.

Ceci nous amène à nous poser la question suivante : une société peut-elle déontologiquement offrir en même temps des services d'audit, de consultance et de renseignement privé ?

L'activité des cabinets qui pratiquent en même temps l'audit, la consultance et le renseignement économique pose, elle aussi, bien évidemment, une série de problèmes éthiques et déontologiques :

- dans quelle mesure d'une part est-il possible d'auditer les comptes d'une société en toute indépendance et, dans le même temps, lui donner des conseils quant à sa stratégie ?
- dans quelle mesure d'autre part un cabinet d'audit peut-il vérifier les comptes d'une entreprise et offrir en parallèle des services en matière de renseignement économique ou concurrentiel à d'autres entreprises sans créer des conflits d'intérêts ?

Les sociétés d'audit ont d'abord soutenu que la deuxième question traduisait l'ignorance des mécanismes qui leur permettent de récolter des informations de sources ouvertes sans recourir à l'espionnage, ni trahir leurs clients. La discrétion absolue à laquelle ces cabinets sont tenus ne souffrirait aucune dérogation et constituerait l'essence même de leur travail.

Cependant la mise en œuvre des nouveaux principes de « Gouvernance d'entreprise » ([85]) a amené certains cabinets d'audit à modifier leur stratégie et à séparer leurs activités d'audit de la consultance.

3.5.7. La normalisation des prestations de renseignement privé.

On constate dans les pays anglo-saxons la mise en place d'associations professionnelles visant à promouvoir des standards de qualité dans l'exercice des professions liées au renseignement privé.

En France, l'Association française de normalisation AFNOR s'est donnée comme mission d'élaborer des normes de référence dont les acteurs socio-économiques ont besoin pour leur développement stratégique et commercial, afin notamment de leur faciliter l'accès aux processus de normalisation. Cette association, reconnue d'utilité publique et placée sous la tutelle du ministère chargé de l'industrie, compte environ 3.000 entreprises adhérentes.

---

[85] Le concept de « Gouvernance d'entreprise » (« *corporate governance* ») s'est développé aux Etats-Unis et en Grande Bretagne en réaction à une série de scandales financiers touchant de grandes entreprises. Ce principe est mis en œuvre par une série de règles législatives, réglementaires, jurisprudentielles et contractuelles qui définissent les modalités de gestion des entreprises. Ce concept est notamment associé à une meilleure surveillance économique, financière et morale du monde économique.

Parmi les nombreuses normes et certifications de produits et de services qu'elle a produites, l'association AFNOR a aussi élaboré une norme expérimentale définissant les différents termes liés à la veille, les différentes caractéristiques des prestations de veille et de mise en place de tels systèmes, leur processus de réalisation, les compétences requises ainsi que les relations entre les clients et les prestataires. Elle s'applique à « *toute prestation concourant à la mise en place et à l'alimentation d'un dispositif de surveillance active de l'environnement technologique, commercial, économique, sociologique, géopolitique, concurrentiel, juridique, réglementaire, normatif, etc., que cette prestation soit réalisée en interne ou en externe, qu'elle fasse l'objet d'une transaction marchande ou non, que l'entité qui la réalise soit publique, parapublique ou privée* » ([86]).

Grâce à ce projet de norme, AFNOR poursuit donc deux objectifs :

- faciliter la relation entre le prestataire interne ou externe à l'entreprise et le client par une terminologie commune, un descriptif de l'offre, une clarification des rôles ou des engagements respectifs ;
- contribuer ainsi à une amélioration de la qualité des prestations.

Il existe en Belgique un Institut belge de la Normalisation (IBN), asbl sous la tutelle du Service public fédéral de l'Economie et de la recherche scientifique. Il a déjà élaboré 15.000 normes ([87]) mais aucune d'entre elles ne concerne encore l'Intelligence économique. Le Comité permanent R a eu connaissance du projet de *l'Institut des Auditeurs de Fraude (a.s.b.l.)* de mettre au point une norme définissant l'objet et l'éthique de la « *Corporate Intelligence* », ses méthodes de travail et d'analyse, de même que les modalités de collaboration entre services privés et instances judiciaires.

4. A QUELLES DIFFICULTÉS SE HEURTE LA PROTECTION DU POTENTIEL ÉCONOMIQUE ET SCIENTIFIQUE DE NOTRE PAYS ?

Le Comité permanent R identifie ici deux difficultés dans la conceptualisation de la mission de protection du potentiel économique et scientifique de notre pays. Il s'agit de la difficulté d'attribuer une nationalité aux entreprises et aux centres de recherche d'une part, de définir et de situer les secrets à protéger d'autre part.

4.1. Comment attribuer un caractère national au potentiel économique et scientifique présent dans notre pays ?

La mondialisation de l'économie constitue une caractéristique nouvelle de notre société. Le pouvoir véritable est désormais détenu par un faisceau de groupes économiques planétaires et d'entreprises globales dont le poids dans les affaires du monde apparaît parfois plus important que celui des gouvernements et des Etats. Par ailleurs, ces restructurations industrielles et la globalisation des procédés au niveau mondial rendent plus difficile l'attribution d'une nationalité aux entreprises. C'est ainsi que des entreprises stratégiques pour le pays peuvent passer sous le contrôle d'investisseurs étrangers. Inversement, une étude récente du bureau d'études commerciales *Graydon Belgium NV* ([88]) révèle que le nombre d'entreprises étrangères passées sous le contrôle de sociétés belges a augmenté de 5,2 % en 2003 pour atteindre les 11.500 unités . Comment déterminer dans ces conditions ce qui constitue le caractère national du potentiel économique ou scientifique à protéger ?

---

86 On peut se procurer ce texte à usage exclusif, moyennant paiement, sur le site www.boutique.afnor.fr
87 Consultables sur le site www.ibn.be
88 Disponible sur http://gateway.graydon.be

Des représentants de la Fédération des Entreprises de Belgique (FEB) ont fait part au Comité permanent R qu'ils considéraient comme belge toute entreprise implantée sur le territoire national et qui y crée une valeur ajoutée, quelle que soit la nationalité de ses actionnaires ou de ses dirigeants.

4.2. Comment définir le secret en matière économique, scientifique et technologique et situer sa place dans une économie caractérisée par les mutations technologiques, la circulation de l 'information et son ouverture internationale ?

Madame Nathalie Rodet-Kroichvilli, chercheuse en économie à l'Université de Technologie de Belfort – Montbéliard (UTBM) analyse la situation de la manière suivante : *« le cadre « traditionnel» de l'économiste, à savoir l'analyse du fonctionnement des marchés, a conduit à une appréhension marginale et souvent très normative de la notion de secret. Les pratiques liées à la détention cachée d'une information sont généralement analysées comme des obstacles au bon fonctionnement des marchés. Le système de prix résultant des mécanismes marchands doit donner à l'ensemble des agents une information pertinente et complète sur l'objet de la transaction. Le secret crée une sorte de fuite d'information qui échappe alors au marché et remet en cause son efficacité. L'économiste de l'innovation en se penchant plus précisément, de par son objet d'étude, sur la nature même de l'information, infléchit quelque peu ce discours normatif : le secret acquiert une certaine légitimité puisqu'il permet à l'entreprise de protéger les résultats de son effort de production d'information et donc agit comme une puissante incitation à produire de l'information. Cependant, l'intérêt collectif est malgré tout mis à mal par cette stratégie. Malgré cette ambiguïté, le secret acquiert un rôle économique.*
Ce n'est que lorsque l'on adopte une vision dynamique des processus concurrentiels, dans le cadre de laquelle la connaissance (et non l'information) devient un enjeu stratégique, que le secret peut acquérir dans une optique non normative le statut de véritable objet de recherche en économie pour qui souhaite étudier les stratégies concurrentielles des firmes. Loin d'être une stratégie parmi d'autres à la disposition des firmes, il est inhérent à toute stratégie. Pour autant, « l'économie du secret » reste un domaine largement inexploré de la science économique et son programme de recherche reste à construire. » ([89])

4.2.1. L'ouverture de la politique scientifique et d'information de l'Union européenne et du gouvernement fédéral.

Il convient en effet de situer la protection des secrets scientifiques et économiques dans le contexte de la mondialisation, de l'ouverture de la politique scientifique de l'Union européenne et du gouvernement fédéral et de la société de l'information et de ses progrès technologiques en général.

89 « *De l'information parfaite au secret : cheminement de l'économiste vers la complexité* » , exposé donné par Mme Nathalie Rodet-Kroichvilli lors du colloque *« Images et usages du secret* » organisé les 6 et 7 novembre 2003 à l'UTBM.

Le premier rapport que le Comité permanent R a consacré à cette matière faisait déjà apparaître la difficulté de sensibiliser les universités et les centres de recherche à la protection de leurs travaux d'autre part : "*Les universités et les centres scientifiques ont toujours été une cible privilégiée en matière de renseignement. L'esprit d'ouverture et le manque chronique de méfiance des chercheurs vis-à-vis de leurs collègues et homologues étrangers ont de tout temps fait de ces centres publics de recherche une cible facile pour les agents des services de renseignement."* ([90])

La déclaration commune des ministres européens de l'Education réunis à Bologne le 19 juin 1999 vise à promouvoir « *l'Europe des Connaissances* » comme « *facteur irremplaçable du développement social et humain* ». A cette fin les ministres se sont engagés à créer un « *espace européen de l'enseignement supérieur* ».

Le sommet des Chefs d'Etats et de Gouvernements de l'Union européenne tenu à Lisbonne en mai 2000 s'est fixé comme objectif stratégique de développer l'économie de la connaissance la plus compétitive et la plus dynamique du monde. A cet égard, l'Union européenne a notamment prévu, à court et à moyen termes, la mise sur pied d'indicateurs européens pour la recherche et le développement, la création d'un grand réseau européen à haute vitesse pour les communications électroniques, la mise sur pied d'un brevet communautaire et la levée de toute entrave à la mobilité des chercheurs. La mise en contact des chercheurs, leur collaboration mutuelle et leur mobilité sont considérées comme des conditions essentielles à la création d'un « *espace européen de recherche* ».
Pour le rendre attrayant aux chercheurs du monde entier, on encourage l'extension des "*Pôles d'attraction technologiques*" (PAT [91]), des "*Pôles d'attractions Inter universitaires*" (PAI [92]), de même que l'octroi de bourses pour les scientifiques des pays tiers. La rencontre de cet objectif, auquel chaque Etat membre a souscrit, nécessite un plan de convergence européen ainsi qu'une coordination des matières scientifiques dans notre pays. *"Seule, en effet, une cohérence globale des efforts de recherche assurera l'indispensable effet de masse permettant à l'Europe de garder une place crédible dans la confrontation qui l'associe aux Etats-Unis et au Japon" ([93]).*

Notons enfin que les accords européens établissant des associations entre les Communautés européennes, leurs Etats membres et certains Etats de l'ancien bloc de l'Est comportent tous un volet relatif à la coopération dans les domaines de la science et de la technologie. Ces accords prévoient notamment des échanges d'informations, l'organisation de réunions scientifiques communes, des programmes communs de recherche et de développement (R & D) qui visent à favoriser le progrès scientifique et le transfert de technologies et de savoir-faire.

Sous l'impulsion du Service public fédéral de l'Economie et de la Recherche scientifique les "pôles d'attraction technologiques" (PAT) et les "Pôles d'attractions Inter universitaires" (PAI) en Belgique ont pour obligation de participer à des équipes de recherche du Nord et du Sud du pays, mais aussi européennes, voire plus largement internationales. De même, des mesures fiscales ont été prises pour favoriser l'accueil de chercheurs étrangers engagés en Belgique dans un post-doctorat ([94]).

---

90 Comité permanent R, rapport d'activités 1998, pages 70 et suivantes.

91 Centres de recherches fédéraux dédiés aux secteurs industriels classiques ou nouveaux pour y stimuler l'innovation.

92 Programmes fédéraux de financement de recherches universitaires.

93 Note d'orientation du ministre de l'Economie et de la Recherche scientifique relative à l'évolution de la politique scientifique fédérale.

94 Note d'orientation du ministre de l'Economie et de la Recherche scientifique relative à l'évolution de lapolitique scientifique fédérale.

A cet égard, la Belgique a, comme tous les pays avancés en la matière, grand intérêt à renforcer l'accueil de chercheurs étrangers afin d'accroître son propre potentiel.

Dans un tel contexte de mondialisation et d'ouverture d'esprit scientifique, la difficulté apparaît clairement de cibler les secrets à protéger pour assurer la pérennité du potentiel scientifique ou économique du pays ainsi que le veut la loi organique des services de renseignement et de sécurité.

4.2.2. La diversification des lieux, des acteurs et des facteurs de puissance.

L'analyse contenue dans la présente section s'inspire des travaux de l'éminent juriste français Bertrand Warusfel, maître de conférences à la faculté de droit de Paris V, auteur d'une thèse sur la protection du secret ([95]). Selon Bertrand Warusfel, la transformation profonde - due pour l'essentiel aux progrès techniques - que connaît notre société "*modifie fondamentalement la valeur des principaux paramètres de l'équation du secret*".

Trois caractéristiques décrivent cette modernité :

- la diversification des facteurs de puissance : à côté des facteurs traditionnels de la puissance politique, diplomatique et militaire, les enjeux de puissance et les luttes stratégiques se déplacent vers l'économie, la technologie et la culture, ce qui conduit à la prise en compte des secrets économiques, scientifiques et technologiques dans les mécanismes légaux de protection du secret;
- la diversification des acteurs de la puissance : à côté des Etats, les acteurs économiques, qu'ils soient nationaux ou supranationaux, jouent un rôle stratégique de plus en plus important;
- la transformation des lieux et des supports de la puissance : la nouvelle donne oppose la délocalisation de la puissance et l'immatérialité des ressources de l'information à l'ancien ordre basé sur la territorialité, la matérialité du pouvoir et l'appropriation physique des ressources. Les moyens et supports du secret sont aujourd'hui essentiellement des systèmes électroniques d'information vulnérables aux manipulations et aux techniques d'interception des communications ([96]).

4.2.3. La mutation des acteurs du secret.

Si donc le contenu du secret évolue, il en va de même aussi bien pour ses producteurs, que pour ses détenteurs, ses protecteurs et ... ses "prédateurs". Alors que le système classique de protection a d'abord été conçu en fonction d'un secret militaire ou d'un secret produit par l'autorité publique, géré par elle et ponctuellement confié à des personnes extérieures "*qui ont besoin d'en connaître"* pour participer eux-mêmes à l'action de cette autorité, la nouvelle réalité économique et stratégique bouleverse le contexte. Celui-ci se caractérise par la diversification et l'hétérogénéité croissante des acteurs, parmi lesquels les entreprises privées novatrices et à forte valeur ajoutée, les laboratoires, ainsi que leurs personnels qui, avec une logique autonome de profit, occupent à présent une place majeure, non seulement dans l'économie marchande, mais aussi dans la recherche scientifique, technologique, les services collectifs, la culture et les relations internationales.

---

95 Bertrand Warusfel, : *Contre-espionnage et protection du secret - Histoire, droit et organisation de la sécurité nationale en France*, juin 2000 - éditions *Lavauzelle.*

96 Lire à ce sujet *"Development of surveillance technology and risk of abuse of economic information"*, by Duncan Campbell - working document for the *Scientific and Technological Options Assessment (STOA)* panel - European Parliament - http://www.gn.apc.org/duncan/stoa.htm

4.2.4. La difficulté de connaître l'ampleur du phénomène de l'espionnage économique.

Les responsables d'entreprises victimes d'actes d'espionnage économique hésitent souvent à porter plainte pour de tels faits. Ils craignent en effet la publicité négative qu'une telle affaire pourrait entraîner pour leur firme ainsi que la perte de confiance des clients, des fournisseurs, des actionnaires, etc.

Dans une enquête effectuée aux Etats-Unis en 1995 par le *National Counterintelligence Center,* 42 % des dirigeants d'entreprises interrogés ont déclaré qu'ils n'avaient jamais signalé de faits d'espionnage aux autorités alors même qu'ils se savaient victimes de tels actes. En outre, même si les responsables de grands groupes industriels reconnaissent qu'ils sont concernés par l'espionnage économique, il ne leur est pas facile de savoir de quelle manière des informations ont été obtenues à leur sujet. Il leur est particulièrement impossible d'affirmer que des marchés ont été perdus en raison d'écoutes et d'interception de leurs communications.

Selon l'avocat Fernand de Visscher, spécialiste du droit de la propriété industrielle, on trouve peu de cas d'espionnage industriel ou commercial dans la jurisprudence belge, la preuve de telles infractions étant difficile à apporter ([97]).

5. LE RÔLE DES SERVICES DE RENSEIGNEMENT OFFICIELS ET PRIVÉS EN MATIÈRE SCIENTIFIQUE ET ÉCONOMIQUE À L'ÉTRANGER.

5.1. Généralités.

Avant de poursuivre plus avant l'examen de la problématique de la protection du potentiel scientifique et économique en Belgique, le Comité permanent R souhaite d'abord examiner en quoi consiste la mission que certains services étrangers ont reçu en cette matière. Plusieurs exemples étrangers seront ici développés permettant de souligner à quel point l'approche du phénomène du renseignement économique et de la protection du potentiel scientifique et économique doit être nuancée et tenir compte des spécificités propres à chaque pays : la France, les Pays Bas, l'Allemagne, le Royaume Uni, le Japon, les Etats-Unis, le Canada, la Russie et Israël.

Quelles missions et quels moyens d'action un gouvernement peut-il donner à ses services de renseignement pour protéger le potentiel scientifique et économique de son pays ? D'autres pays que la Belgique ont confié à leurs services de renseignement la mission de protéger leur potentiel scientifique ou économique. Cette mission peut se concevoir de manière défensive et de manière offensive. Quels rôles jouent les services de renseignement privés en cette matière ?

[97] La libre Belgique 16 janvier 2001 page 15 : "*Que les espions lèvent le doigt ...*"

Durant les longues années de la guerre froide, la préoccupation des services de renseignement était la recherche d'information macro-économique pour comprendre les grandes tendances de l'économie mondiale et anticiper ses évolutions. Les services de renseignement du monde entier ont déployé une part considérable de leurs activités à se poser des questions sur le fonctionnement des systèmes économiques dans les pays communistes.

A lire la littérature consacrée à l'action de ces services à cette époque, ceux-ci n'auraient pourtant pas été en mesure d'apprécier correctement la situation économique de ces pays. Par exemple, le produit intérieur brut de l'URSS, ses capacités de production et sa situation financière auraient été largement surévaluées, d'où l'incapacité de prévoir l'effondrement final du système communiste à partir de 1989.

Aujourd'hui, la nature de la prospective économique a changé. L'utilisation des services officiels de renseignement pour promouvoir les activités économiques de la nation est devenue une réalité. Des pays comme le Japon et les Etats-Unis concentrent leurs efforts sur des marchés et des zones à fort potentiel de croissance. Certains pays européens comme l'Allemagne et la France leur emboîtent le pas dans cette direction.

Par ailleurs, chacun de ces pays favorise également le développement de projets en matière de veille ou d'intelligence économique dans les entreprises. Ces stratégies d'intelligence économique menées au niveau national s'articulent souvent sur des projets de développement territorial ainsi que sur des réseaux locaux de partage d'expertise et d'informations qui associent entreprises privées (sans négliger les PME), autorités locales et régionales, administrations publiques, associations professionnelles, centres de recherches et autres partenaires concernés par le développement économique.

5.2. En France.

5.2.1. La législation.

La loi du 16 juillet 1980 réprime notamment toute communication à une autorité publique étrangère, *"de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public, précisés par l'autorité administrative en tant que de besoin".* Selon l'article 410-1 du code pénal français de 1992, les intérêts fondamentaux de la Nation se caractérisent par : son indépendance, l'intégrité de son territoire, sa sécurité, la forme républicaine de ses institutions, les moyens de sa défense, sa diplomatie, la sauvegarde de sa population, l'équilibre de son milieu naturel et de son environnement, les éléments essentiels de son potentiel scientifique et économique et son patrimoine culturel.

Les dispositions du code monétaire et financier relatives aux investissements étrangers en France prévoient qu'un tel investissement doit faire l'objet d'une autorisation préalable de la direction du Trésor s'il « *est de nature à mettre en cause l'ordre public, la sécurité publique ou encore la santé publique* » ou bien s'il est « *réalisé dans des activités de recherche, de production ou de commerce d'armes, de munitions, de poudres et substances explosives destinées à des fins militaires ou de matériels de guerre* ». Le rapport du député Carayon ([98]) propose d'élargir ce système de contrôle aux « *technologies de souveraineté et services de confiances*».

[98] Voir point 5.2.3. ci-après

La loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications prévoit des motifs qui justifient la conduite d'interceptions administratives de communications. Parmi ces motifs, on trouve le terrorisme, la criminalité organisée, la sécurité nationale, mais aussi la sauvegarde du potentiel économique et scientifique. Au cours de ces dernières années cependant, le nombre d'interceptions de sécurité autorisées en France à des fins de sauvegarde du potentiel économique et scientifique n'a cessé de décroître au profit des interceptions motivées par le terrorisme et la criminalité organisée. En 2001, les interceptions motivées par des fins de sauvegarde du potentiel économique et scientifique ne représentaient plus que 1,5 % des demandes initiales et 1 % des renouvellements ([99]).

En mars 2003, la loi n° 83-629 du 12 juillet 1983 réglementant les activités privées de sécurité (activités privées de surveillance et de gardiennage, de transport de fonds et de protection des personnes) a été complétée par un titre II relatif aux « *agences de recherches privées* » ([100]). Cette loi définit l'activité privée de recherche de renseignements et d'informations pour compte de tiers comme étant une profession libérale ([101]) exigeant une certaine qualification professionnelle et soumet l'exercice à titre individuel de cette profession à une procédure d'agrément. En outre, le personnel employé pour exercer une telle activité doit être déclaré auprès d'un préfet.

L'autorisation peut être retirée « *à la personne physique ou morale dont l'activité porte atteinte à la sécurité publique, à la sûreté de l'Etat ou aux intérêts fondamentaux de la nation dans les domaines économique, scientifique, industriel ou commercial*. » La surveillance des personnes exerçant des activités privées de recherche est confiée aux autorités de police.

5.2.2. L'action du Chef de l'Etat et du gouvernement.

Un décret du Président de la République a créé le 1er avril 1995 un **Comité pour la compétitivité et la sécurité économique** (CCSE) d'abord placé sous l'autorité du Premier ministre, puis sous celle du ministre de l'Economie, des Finances et du Plan et dont le Secrétariat Général de la Défense Nationale (SGDN) assure le secrétariat. Composé de sept membres, le CCSE était chargé de mettre en oeuvre les recommandations du rapport "Martre" en matière d'intelligence économique. Ce Comité a cependant échoué dans sa mission et il a été mis fin à son existence en juillet 1998.

Un rapport de 1997 rédigé par le **Commissariat général du Plan** et intitulé *"de la défense économique à la sécurité de l'économie"* examine quels devraient être "*les leviers offensifs de l'Etat dans le domaine de la sécurité économique*". Il prône notamment le renforcement des pouvoirs du gouvernement afin qu'il puisse s'opposer à des acquisitions stratégiques, l'établissement de sanctions pénales en cas d'infraction au secret d'entreprise, la définition d'une politique nationale des normes et brevets, l'organisation d'un réseau de veille technologique et concurrentielle ciblé sur des thèmes stratégiques, le développement de stratégies d'influences offensives et enfin l'accroissement des capacités d'enquête de la Police judiciaire, des Renseignements généraux, de la DST et des Douanes en matière de criminalité économique.

---

99 Commission nationale de contrôle des interceptions de sécurité - 10ème rapport d'activité 2001.

100 Article 102 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure (http://www.legifrance.gouv.fr/).

101 Le statut de « profession libérale » n'est pas défini mais cette mention dans la loi résulte probablement de la prise en compte par le législateur français d'une demande des professionnels de ce secteur que soit reconnue l'indépendance qu'ils revendiquent. Des considérations fiscales ont aussi été prises en compte.

Une circulaire du ministre de l'économie, des finances et de l'industrie datée du 14 février 2002 a pour objet de présenter les différents aspects de la défense économique et de décrire son organisation aux niveaux national, zonal, régional et départemental avec les responsabilités afférentes. Au même titre que la défense nationale et la défense civile, la défense économique constitue l'une des trois composantes de la défense de la Nation ([102]).

5.2.3. La mission parlementaire sur l'intelligence économique.

Au début de l'année 2003, le Premier ministre français, M. Jean-Pierre Raffarin a commandé un rapport parlementaire sur l'état de l'intelligence économique en France. Il a confié cette mission à un député du Tarn, M. Bernard Carayon, membre de la commission des finances de l'assemblée nationale. La demande du Premier ministre était ainsi libellée : « *dresser un état des lieux de la façon dont notre pays intègre la fonction d'intelligence économique dans son système éducatif et de formation, dans son action publique et au sein du monde des entreprises ; mettre en exergue les éventuelles carences en ce domaine ; faire les recommandations nécessaires à la valorisation de la fonction d'intelligence économique en ce compris les recommandations utiles au développement de la sensibilisation à ces sujets, dans tous les secteurs qui paraîtraient pertinents, en mettant l'accent sur le troisième cycle universitaire, les grandes écoles, les entreprises des filières stratégiques,*

sans oublier les services publics concernés ; étudier les moyens de promouvoir les métiers de l'intelligence économique au sein des sphères publique ou privée ; établir les conditions dans lesquelles les pouvoirs publics, seuls ou avec d'autres intervenants notamment privés, pourraient optimiser la coordination de l'intelligence économique, définir une stratégie et une planification dans ce domaine et s'assurer de l'utilisation effective de ces données par les acteurs intéressés. »

Le député Carayon a remis son rapport au Premier ministre français au mois de juillet 2003. Ce document a été rendu public dés le mois de septembre 2003 ([103]). Ce document intitulé « ***Intelligence économique, compétitivité et cohésion sociale*** » présente un panorama de l'intelligence économique et France et comporte 38 recommandations destinées à valoriser cette fonction. Selon le député rapporteur, l'Intelligence économique devrait être « ***une vraie et grande politique de l'Etat*** *à l'instar de ce que sont les politiques de santé, d'environnement ou de fiscalité*. » « *Que cette politique soit nationale, décentralisée ou internationale, elle ne pourra s'épargner un effort de formation et d'information calibré à cette ambition et adapté à une certitude :* ***l'intelligence économique est un patriotisme économique*** », c'est-à-dire « ***une politique sociale*** ». Mais le rapport constate pourtant un défaut de sensibilité de l'État aux questions de sécurité. Ainsi l'Etat n'a jamais défini ni les secteurs d'activités stratégiques, en termes de souveraineté, d'emplois, d'influence, ni les technologies dures s'y rattachant, et n'a jamais évalué les forces et les faiblesses de la recherche et des industries françaises dans les dits secteurs. *«La culture du renseignement reste étrangère aux mentalités de nos élites »* regrette Bernard Carayon. Par ailleurs, le rapport pose clairement l'existence des sociétés de renseignement privé (SRP) comme problème de sécurité nationale : « *la nature même de leur métier exige des précautions particulières ; leur activité n'est pas neutre au regard du respect des libertés publiques ; les entreprises ont besoin de partenaires de confiance présentant des garanties d'éthique, de confidentialité et de professionnalisme* ».

---

[102] Journal Officiel n° 70 du 23 mars 2002, page 5164.

[103] www.ladocfrancaise.gouv.fr/BRP/034000484/0000.pdf

Parmi les 38 propositions développées dans le rapport Carayon, on peut notamment mentionner :

- La définition d'un « périmètre stratégique » des « « *technologies de souveraineté et services de confiances*» (aérospatial, défense, informatique, télécommunications, pharmacie, etc.) avec un système de contrôle des investissements étrangers élargi à ces secteurs,
- La création d'un Conseil national pour la compétitivité et la sécurité économique (CNCSE) composé de personnalités du monde économique et scientifique, présidé par le Premier ministre, et dont le rôle serait notamment d'alerter le gouvernement,
- La création d'un Centre d'analyse et de prévision (CAP) interministériel et la nomination d'un délégué interministériel à la compétitivité et à la sécurité économique,
- La création d'une cellule de contact et de soutien aux entreprises,
- Le développement d'un enseignement universitaire adapté aux besoins,
- La mise en place et la promotion de réseaux au niveau régional et local,
- **La confirmation et le renforcement du rôle des services de renseignement**, notamment la Direction de la Surveillance du Territoire (DST), la Direction Centrale des Renseignements Généraux (DCRG) et la Direction Générale de la Sécurité Extérieure (DGSE), en matière de protection du potentiel scientifique et économique, en collaboration avec d'autres ministères et services de police,
- La mise en place d'une mission interministérielle d'expertise technique et industrielle des systèmes d'information des administrations publiques.

Les conclusions et les propositions avancées par ce rapport devraient logiquement orienter la politique du gouvernement français en matière d'intelligence économique dans les prochaines années.

5.2.4. L'action des autorités territoriales décentralisées et des Chambres de Commerce et d'Industrie (CCI).

Aujourd'hui, certaines autorités territoriales décentralisées (préfets, conseils régionaux, conseils généraux, conseils municipaux, etc.) encouragent le développement de «pôles d'excellence», c'est-à-dire de partenariats entre entreprises, chambres de commerce et d'industrie, centres de recherche publics ou privés, universités et grandes écoles et consultants privés afin de favoriser le développement économique de leur région ou celui d'un secteur d'activités particulier.

Dans ce contexte, certaines Chambres de Commerce et d'Industrie développent des initiatives en matière d'intelligence économique afin de participer à la production de connaissances utiles aux stratégies d'entreprises, contribuer à la sécurité du patrimoine des entreprises et des échanges électroniques, ainsi qu'au développement de stratégies d'influence. Le rapport « ***Intelligence économique, compétitivité et cohésion sociale*** » présente un inventaire des initiatives prises en ce sens et il propose que les régions soient considérées comme territoires de référence de l'intelligence économique. On parle ici de systèmes locaux ou territoriaux d'intelligence économique. Cinq régions pilotes ont d'ailleurs été désignées récemment par le gouvernement français.

5.2.5. Le rôle des services de renseignement français en matière de protection du potentiel scientifique et économique.

Le rapport du député Carayon identifie le rôle des quelques services de police, de renseignement et de sécurité en matière de protection de l'économie, notamment les services suivants :

- **La Direction Générale de la Gendarmerie Nationale (DGGN)** : « *par sa présence dans les zones rurales, (elle) peut recueillir, à l'occasion de ses missions traditionnelles, de nombreuses informations relevant de la sécurité économique. (…) (Elle) dispose d'un vrai maillage territorial, en particulier dans des zones de fortes implantations de PMI/PME. Surtout, la Gendarmerie participe déjà activement à la protection des infrastructures vitales et critiques (centrales nucléaires, etc.)* ».

- **La Direction Centrale des Renseignements Généraux (DCRG)** est un service de police qui dépend du ministre de l'Intérieur et qui est chargé de la recherche et de la centralisation des renseignements d'ordre politique, social et économique nécessaires à l'information du Gouvernement. Il assure la police de l'air, le contrôle des personnes aux frontières et la surveillance des établissements de jeux et des champs de courses (Article VII du décret présidentiel n 67-196 du 14/03/1967). La DCRG est aussi chargée de la recherche et de la centralisation des renseignements destinés à informer le Gouvernement; elle participe à la défense des intérêts fondamentaux de l'Etat; elle concourt à la mission générale de sécurité intérieure (Article 3 du décret du premier ministre n 95-44 du 16/01/1995). *« Par son suivi des phénomènes de société, son maillage territorial et ses effectifs, (elle) peut également participer à cette mission de protection économique ».*

- **La Direction Générale des Douanes et des Droits Indirects** qui est en première ligne dans la lutte contre les contrefaçons.

- **La Direction Générale de la Sécurité Extérieure (DGSE)** remplit à l'étranger une mission de contre-espionnage et de contre-influence. Selon Bernard Carayon, cette mission n'a pas encore été suffisamment reconnue comme prioritaire par l'Etat. La DGSE organise des séminaires destinés aux chefs d'entreprises afin de les informer et de les sensibiliser aux diverses activités de renseignement menées en France au préjudice de la collectivité nationale.

- **La Direction de la Protection et de la Sécurité de la Défense (DPSD)** a pour mission d'assurer la protection du secret, la sécurité des forces armées et celle des points sensibles militaires parmi lesquels les entreprises intéressant la Défense nationale ([104]). La DPSD développe également une activité d'analyse des risques liés aux partenariats industriels et commerciaux, aux attaques informatiques et aux implantations territoriales douteuses.

- **La Direction de la Surveillance du Territoire (DST) :** les missions de la DST étant assez proches de celles de la Sûreté de l'Etat en Belgique, celles-ci seront examinées ici plus en détail.

[104] En Belgique, ce type de mission est assuré par le SGRS.

- Un décret du 22 décembre 1982 définit la mission de la Direction de la Surveillance du Territoire (DST), service français de sécurité intérieure comme étant la lutte contre les activités inspirées, engagées ou soutenues par les puissances étrangères de nature à nuire à la sécurité ou aux intérêts fondamentaux du pays. Son activité principale est la recherche du renseignement de sécurité afin de protéger le pays contre les menaces d'origine étrangère, quelles qu'en soient les formes.

- L'action de la Direction de la surveillance du territoire (DST) en matière de protection du potentiel scientifique et économique est décrite comme étant une "*tâche de sensibilisation qui consiste, avec une inlassable persévérance, à informer, à mettre en garde tous ceux qui, dans leur domaine technique, scientifique, économique, administratif, militaire ou même politique, peuvent être, à un moment donné, des cibles pour les services spéciaux étrangers*"; une des priorités dans cette tâche de sensibilisation concerne les chefs d'entreprises dont les réalisations risquent d'être menacées par les différentes formes de l'espionnage économique. "*Sur le terrain, des actions de sensibilisation sont donc menées jusque dans les usines et les laboratoires notamment par le biais d'exposés informatifs visant, au moyen d'exemples commentés, à présenter les moyens d'investigation clandestine pouvant être mis en oeuvre par tout service de renseignement moderne ou, plus simplement, par un visiteur mal intentionné*" ([105]). Ces séances d'informations s'adressent aux responsables administratifs, aux cadres commerciaux, aux directeurs de marketing, etc., mais aussi aux secrétaires car elles (ils) sont des objectifs intéressants pour les services adverses : elles prennent connaissance de tout ce qui passe sur le bureau de leur patron et contrôlent souvent certains moyens de reproduction, telles les photocopieuses. On met l'accent sur la nécessaire responsabilisation de tout acteur détenant une parcelle de connaissance spécifique. La protection des usines et des laboratoires passe également par l'établissement d'un partenariat entre la DST et les organismes concernés pouvant aller jusqu'à la réalisation d'un véritable "audit de sécurité". Ces "radiographies" visent principalement à délimiter le "noyau dur" à protéger, à identifier les "domaines d'avidité" susceptibles d'intéresser les tiers malveillants et à indiquer les méthodes adaptées pour se protéger de toute ingérence.
  Mais ces missions de sensibilisation et d'audit n'aboutissent jamais à opérer un transfert de responsabilité. Le rôle du service est de dresser un bilan et de porter les conclusions à la connaissance des responsables de l'entreprise ou du laboratoire qui sont ensuite libres de prendre ou non les mesures adaptées.

  Pour respecter cette règle du jeu, les fonctionnaires de la DST ont adopté trois garde-fous : pas de substitution au service de sécurité, pas d'intrusion et pas d'interférence dans les affaires socioprofessionnelles.

[105] "*Le renseignement français à l'aube du XXI e siècle"* de Jean-Jacques Cécile éditions Lavauzelle – 1998, pages 36 & suivantes.

Par ailleurs, l'implication de la France au sein de l'Europe, la mise en place de règles supranationales, qui s'imposent aux lois internes, pousse la DST à prendre en compte cette nouvelle dimension dans l'exercice de sa mission. La création de groupes industriels européens - par exemple, le consortium EADS ([106]) - conduit la DST à envisager une protection patrimoniale qui doit s'étendre au-delà du territoire français. Dans cette optique, la DST envisage d'établir des partenariats avec des services homologues européens. La DST n'oublie cependant pas que ses partenaires dans certains domaines, sont aussi ses concurrents dans d'autres. Enfin, la DST considère qu'elle doit s'intéresser aux atteintes que pourraient subir les organismes de l'Union européenne à Bruxelles de la part d'Etats non-membres. Elle s'attache à suivre les luttes d'influences, entre européens, au sein des différentes instances de l'Union.

La DST est également attentive au phénomène « d'atomisation » et de « privatisation » de la menace, qui rend difficile à la fois son identification et sa neutralisation. Ce phénomène se manifeste notamment par la reconversion, dans le secteur privé, d'anciens officiers de renseignement, ainsi que par l'émergence ou le renforcement de nouveaux types d'activités qui rendent moins sûr l'environnement de l'entreprise. Et la DST de citer les sociétés de renseignement privées, les cabinets d'audit ou de consultants, les compagnies d'assurances, les organismes de traduction et d'interprétariat, les firmes de sous-traitance et de maintenance des systèmes informatisés. Concrètement, la mission de protection du patrimoine de la DST s'exerce dans le cadre d'un étroit partenariat avec les principaux acteurs économiques nationaux et elle s'articule autour de deux missions complémentaires que sont la lutte contre la prolifération et les enquêtes menées en matière de sécurité et de compromission des documents classifiés « Confidentiel Défense », « Secret Défense » et « Très Secret Défense ».

Un sondage d'opinion publié le 25 novembre 2003 par le journal « *Veille magazine* » semble indiquer une adhésion globale des français à l'implication des services de renseignement d'Etat dans la démarche de l'intelligence économique ([107]).

5.3. Les Pays-Bas.

Il est intéressant d'observer l'action des services de renseignement d'un pays voisin de taille et de potentialité scientifique ou économique comparable à la Belgique.

---

106 Le consortium européen EADS (*European Aeronautic Defence and Space Company*) est le numéro 2 mondial de l'industrie aéronautique et de défense, employant environ 100.000 personnes principalement en France, en Allemagne, en Grande Bretagne et en Espagne. EADS occupe aussi des positions de premier plan sur le marché des satellites et des avions militaires de transport militaire, de mission ou de combat. EADS résulte de la fusion en juillet 2000 *d'Aérospatiale Matra* (FR), de *Daimler Chrysler Aerospace AG (Dasa)* (RFA) et de *Construcciones Aeronauticas SA (CASA)* (Esp.)

107 Disponible sur http://www.veillemag.com/

Jusqu'il y a peu, les Pays-Bas ont disposé d'un service de renseignements extérieurs, « *de inlichtingendienst buitenland (IDB) »*, dissout en 1994. Selon Bob de Graaf et Cees Wiebes, auteurs d'un ouvrage intitulé "*Villa Maarheeze"* ([108]), l'IDB possédait une section économique chargée de collecter des renseignements en faveur du ministère des Affaires économiques, de l'Agriculture et de la Pêche. Le recueil du renseignement s'effectuait principalement via des hommes d'affaires néerlandais voyageant ou séjournant à l'étranger. L'IDB entretenait aussi des contacts avec la direction des grandes entreprises hollandaises avec lesquelles il échangeait des informations d'ordre économique de première importance. Selon de Graaf et Wiebes, l'IDB aurait intercepté des offres commerciales étrangères transmises par télécommunications pour les communiquer à des entreprises nationales.

Après la dissolution de L'IDB, ses opérations ont été transférées au *Binnenlandse Veiligheids Dienst* (BVD, homologue néerlandais de la Sûreté de l'Etat), dont les missions légales ont été définies comme suit :

- collecter des renseignements sur des organisations et personnes qui, par les buts qu'elles se fixent ou par leurs activités, permettent de supposer sérieusement qu'elles représentent un danger pour la démocratie, la sécurité ou pour d'autres intérêts vitaux de l'Etat;
- exécuter des enquêtes de sécurité;
- favoriser des mesures de protection des données dont la confidentialité s'impose dans l'intérêt de l'Etat, des secteurs des pouvoirs publics et du monde économique et qui sont de l'avis des ministres compétents, d'un intérêt vital pour le maintien de la vie en société.

Cette définition large des missions inclut la protection de l'économie nationale. Dans ce cadre, le BVD enquête sur les activités des services de renseignement étrangers dirigées contre les intérêts économiques des Pays-bas. Dès sa création le BVD a rempli une mission de sécurité, particulièrement à l'égard des entreprises travaillant pour l'armée et de celles qui pourraient être victimes de sabotage. La loi hollandaise sur les services de renseignement autorise le BVD à attirer l'attention des entreprises sur les mesures de protection à prendre. Ce service peut également signaler certaines formes de concurrence illicite. En 1994, la mission du BVD relative au domaine économique a été redéfinie comme suit par un groupe "*Economische Veiligheidsbelangen*" (Intérêts de sécurité économique) associant le ministère des Affaires économiques et des représentants d'entreprises.

1. les entreprises disposent d'un éventail important d'informations qui sont la proie de l'espionnage économique;

2. des marchés ne sont pas obtenus par les firmes néerlandaises car les concurrents étrangers de ces firmes utilisent des moyens peu avouables tels que des écoutes ou des informateurs pour gagner ces marchés;

3. il est indispensable de mener des enquêtes sur la fiabilité d'entreprises et d'investisseurs qui entretiennent des rapports avec le crime organisé.

Il a donc été décidé que les activités du BVD devaient porter sur ces trois menaces spécifiques. Le BVD s'occupe aussi de menaces telles que :

- le recueil par des services de renseignement étrangers de données économiques essentielles concernant des firmes néerlandaises;

---

[108] *Geschiedenis van de inlichtingendienst buitenland - Sdu uitgeverij, Den Haag - 1999.*

– le lancement de campagnes de presse calomnieuses dans le but de discréditer des entreprises néerlandaises.

Le ministre de l'Intérieur a établi une liste confidentielle des entreprises présentant un intérêt vital pour les Pays-Bas et dont le BVD doit assurer la protection.

Les Pays-Bas semblent donc avoir adopté une politique purement défensive mais qui associe de manière active le monde économique et le monde politique.

Au cours de l'année 2002, le « *Binnenlandse Veiligheidsdienst* » (BVD) s'est transformé en « *Algemene Inlichtingen- en Veiligheidsdienst* » (A.I.V.D.) ou « Service général du renseignement et de la sécurité ». Ce nouveau service a conservé les compétences du BVD en matière de protection du potentiel scientifique et économique. Selon le rapport d'activité 2002 de l'A.I.V.D. ([109]), les services de renseignements russes sont toujours très actifs dans les pays d'Europe de l'Ouest afin de recueillir des informations d'ordre scientifique et économique. Comme la D.S.T., l'A.I.V.D. situe essentiellement sa mission en matière de protection du potentiel scientifique et économique sur le plan préventif. Ce service associe aussi cette mission à la lutte contre la prolifération d'armes de destruction massive. Il tente donc de s'opposer à l'acquisition par des services de renseignement étrangers ou par des groupes terroristes, via le territoire néerlandais, de connaissances ou de matériels susceptibles de favoriser le développement de telles armes. L'A.I.V.D. informe donc les secteurs économiques et scientifiques concernés sur la manière d'éviter de contribuer à la prolifération d'armes de destruction massive. L'A.I.V.D. a annoncé qu'il mènerait une enquête en 2003 sur les atteintes possibles que des services de renseignement étrangers font courir à la position économique concurrentielle des Pays-Bas.

5.4. L'Allemagne.

L'Allemagne s'est lancée très tôt dans la recherche de renseignements d'ordre scientifique et économique. En 1915, au cours de la première guerre mondiale, S. Herzog, un ingénieur conseil allemand publie un livre intitulé « *Le plan de guerre commerciale de l'Allemagne* » dans lequel il expose la stratégie que ce pays doit entreprendre afin de conforter sa victoire militaire par la maîtrise commerciale du monde. Dans ce plan, l'organisation du système de renseignement allemand est présentée comme un élément essentiel du succès. Elle devra donc être poussée le plus loin possible. Ce plan de guerre intègre la dimension opérationnelle de la circulation de l'information à tous les niveaux de l'action. Les représentations diplomatiques y sont décrites comme l'avant-garde de la guerre d'exportation car elles détectent toutes les attitudes hostiles des autres pays. Tous les Allemands établis à l'étranger sont appelés à se mobiliser pour la défense des intérêts économiques du IIème Reich : « *On tiendra les statistiques les plus détaillées sur les matières et des fiches de renseignement sur les personnes ; on suivra toutes les inventions et perfectionnement techniques réalisés à l'étranger pour les porter à la connaissance des industriels allemands qu'ils peuvent intéresser* ». L'acheminement des informations récoltées à l'étranger doit être assuré par des relais nationaux comme les fédérations professionnelles et les Chambres de Commerce et d'Industrie. Ce plan, qui fait la part belle au renseignement économique, a été lu avec attention par le président américain Hoover ; ce document inspire toujours aujourd'hui la stratégie économique et commerciale, non seulement de l'Allemagne mais aussi celle d'autres pays comme les Etats-Unis ([110]).

---

[109] Algemene Inlichtingen- en Veiligheidsdienst (A.I.V.D) Jaarverslag 2002, p.. 57 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

[110] C. Harbulot et J. Pichot-Duclos – *La France doit dire non !* Infoguerre.com avril 2003. Le rapport Herzog a été réédité en 2003 par la maison d'édition française Lavauzelle (www.lavauzelle.com).

Il n'est donc pas étonnant que, selon Henri Martre, rapporteur pour le Commissariat général du Plan français ([111]), le système d'intelligence économique le plus performant en Europe soit le modèle allemand. Celui-ci s'appuie avant tout sur un profond sentiment collectif de "patriotisme économique" et un consensus sur la notion d'intérêt économique national. Cette culture est un des atouts de la compétitivité allemande.

Le *"Bundesnarichtendienst"* (BND), c'est-à-dire le service de renseignement extérieur de la RFA, serait le centre vers lequel converge l'ensemble des flux d'informations économiques ([112]). Le gouvernement allemand considérant l'Asie comme une zone prioritaire en termes stratégiques pour le redéploiement des forces, tant sur le plan économique que sur celui du renseignement, ce n'est pas un hasard si le BND a ouvert des postes à New Delhi, à Pékin, à Djakarta, à Tokyo, à Manille, à Séoul et à Taiwan. Le BND a mis en place une banque de donnée pour les entreprises qui s'implantent dans ces régions du monde ([113]). Le BND rédige aussi des rapports à l'intention du ministère fédéral de l'Economie, notamment pour inviter les industriels allemands à la vigilance dans leurs relations avec certains pays cherchant à acquérir des systèmes de haute technologie. Il existe également un organisme fédéral chargé de coordonner les initiatives dans le domaine de l'intelligence économique : l'*"Arbeitsgemeinschaft für die Sicherheit des Wirtschaft"* (ASW). Cet organisme entretient des contacts avec le service fédéral de renseignement, le *"Bundesampt für Verfassungsschutz"* (l'office de protection de la Constitution ou BfV).
Selon un rapport du BfV de 1997, 62 % des affaires d'espionnage mises à jour en Allemagne concernent le potentiel scientifique et économique du pays, 19 % concernent des affaires politiques et administratives, 8 % se situent dans le domaine militaire et 11 % dans d'autres secteurs. Des activités d'espionnage commanditées par des services de renseignement russes à l'encontre d'entreprises privées allemandes seraient en nette augmentation. Le rapport annuel du BfV de 1999 confirme que les activités du service de renseignement extérieur russe, le SVR, ainsi que des pays de la CEI sont principalement orientées vers l'espionnage économique, scientifique et technique.

Dans un entretien accordé au mensuel français "*Le Monde du Renseignement"* ([114]), M. Peter Frisch, le chef du BfV déclare que la notion de "*patrimoine économique stratégique"* a conduit une partie des 2218 agents du BfV à choisir certaines entreprises afin de développer des collaborations avec elles. A ce jour, elles sont 1600 à avoir établi des partenariats avec le BfV au niveau fédéral. Dans chacune d'elles, un salarié assure des fonctions de délégué à la sûreté économique et de correspondant pour le service de renseignement. Les sociétés concernées appartiennent, non seulement à l'industrie de l'armement, mais aussi à la construction automobile, à la pétrochimie et aux secteurs des hautes technologies. Ce dispositif est doublé par un réseau régional, avec de semblables partenariats gérés par les *"Landesamt fûr Verfassungsschutz"*, c à d les services de renseignement des länder. Le BfV entretient des contacts avec des firmes et des institutions de recherche afin de les informer sur les programmes d'armement poursuivis par certaines puissances étrangères. Ce service indique quelles sont les technologies et les savoir-faire recherchés par les services de renseignement étrangers et sensibilise ses interlocuteurs sur les risques encourus lorsqu'ils sont en relation avec certaines firmes ou centres de recherche étrangers.

---

111 Henri Martre : *Intelligence économique et stratégie des entreprises,* la documentation française.
112 DST, police secrète - Roger Faligot, Pascal Krop - Flamarion
113 *Une approche française de l'intelligence économique* - Christian Harbulot - novembre 1995
114 Le Monde du Renseignement n° 375, 3 février 2000.

5.5. La Grande Bretagne

La pratique de l'intelligence concurrentielle de même que la culture offensive du renseignement économique est bien ancrée dans les grands groupes industriels britanniques (par la création de « war rooms » par exemple). Les PME sont elles aussi initiées à cette démarche via les « Business Links », véritables réseaux territoriaux d'appui et de diffusion d'informations à haute valeur ajoutée (export, innovations technologiques, appels d'offres, etc.). Chaque région de Grande Bretagne dispose de son « Business Link » ([115]).

Par ailleurs, la législation anglaise assigne une mission de protection de l'intérêt du bien-être économique du Royaume-Uni tant pour le Security Service (act 1989) que pour "*The Secret Intelligence Service (act 1994)* ([116]). Aucune des deux lois ne définit le concept de bien-être économique (*economic well being)*. Le "*Government Communications Head Quarter" (GCHQ)* est spécialement chargé par la loi d'intercepter des communications étrangères pour le compte du gouvernement, notamment "*... in the interest of the economic well-being of the United Kingdom ... in relation to the actions or intentions of persons outside the British Islands".* Des cibles économiques et commerciales peuvent être désignées par le *"Overseas Economic Intelligence Committee"* du gouvernement, par la section économique du "*Joint Intelligence Committee"* et même par le Trésor et la Banque d'Angleterre. Les ministres concernés doivent désigner les entreprises clés pour l'économie britannique. Ils donnent des directives par le canal du "*Joint Intelligence Committee*" (JIC). Ils demandent, par exemple, aux services de renseignement de s'informer sur la manière dont le prix du pétrole va varier de manière à permettre au ministre d'adapter sa politique financière.

Les services de renseignement travaillent donc pour l'Etat à qui ils diffusent les informations et non aux entreprises. Le JIC donne des directives aux services de renseignement après discussion avec les ministres et consultation des entreprises. Les relations qui existent entre les services de renseignement et les entreprises sont des relations humaines sans structure comme support.

5.6. Le Japon.

Pour des raisons historiques et culturelles, le Japon occupe une place à part : l'économie y a pris rang de priorité absolue. Lorsqu'il s'est ouvert au monde, à partir des débuts de l'ère Meji en 1867, ce pays a accordé au traitement de l'information technologique et industrielle une importance nationale, en la considérant comme une ressource à exploiter de manière collective. Dans la Constitution du Japon, on peut d'ailleurs lire : « *Nous irons chercher la connaissance dans le monde entier afin de renforcer les fondements du pouvoir impérial* ».

Il est par ailleurs intéressant de noter que le Japon est passé du modèle de développement économique tiré par l'imitation au modèle tiré par la découverte et l'innovation.

---

115 Voir www.businesslink.org sur le site du *Department of Trade and Industry* du Royaume Uni.

116 "*Etude de la législation du Royaume-Uni relative aux services de renseignement et de sécurité*", rapport annuel d'activités du Comité permanent R 1998.

L'appareil de renseignement privé au Japon s'est fondé et a grandi en s'appuyant sur des confréries nationalistes ([117]). Cette tendance était d'autant plus naturelle que la distinction entre intérêt particulier et intérêt de la nation était, dans le Japon du XIXème siècle, quasiment inexistante et qu'il était naturel que l'individu s'y efface devant le collectif. Cette genèse explique pourquoi, aujourd'hui, le renseignement « privé » au Japon est mené par des associations ou des conglomérats d'entreprises – voire par des fédérations industrielles – et que les sociétés privées spécialisées y sont rares.

Ce pays a en effet développé un système global de collecte d'informations dans lequel chacun, du simple citoyen (et, a fortiori, de l'employé de base) jusqu'aux responsables gouvernementaux, est susceptible de collecter des renseignements. Le touriste japonais qui photographie tout et ramène sa moisson d'information à son patron n'est donc pas totalement un mythe : la plupart des entreprises japonaises encouragent, financièrement mais aussi par des promotions ou des voyages, les employés qui ramènent au bureau des idées intéressantes et applicables au marché japonais glanées à l'étranger ». Cette pratique est appelée « rapport d'étonnement ».

Au niveau plus élevé et plus organisé, de grandes sociétés de négoce (les « *Sogo Shosha*»), certaines sectes d'inspiration shintoïste et des associations professionnelles pratiquent la collecte intensive du renseignement économique et industriel utile au Japon.

L'Etat nippon se consacre donc tout entier au service de ses entreprises et des priorités économiques, au point d'y consentir des efforts sans commune mesure avec ce qui se passe ailleurs dans le monde. Certains ouvrages évaluent à 480 milliards de francs belges le budget de la recherche d'informations au Japon ([118]) essentiellement financé par le secteur privé. C'est ainsi que le ministère du Commerce et de l'Industrie (*MITI - Ministry of International Trade and Industry*) dispose d'une organisation spécialisée dans le renseignement économique et commercial, le JETRO (Japanese External Trade Organisation), qui entretient plusieurs dizaines de bureaux à l'étranger, pour l'essentiel voués à la recherche de l'information et, au-delà, du renseignement. L'Agence des sciences et des techniques (STA), chargée de la recherche scientifique sous la tutelle du premier ministre, octroie de nombreuses bourses pour permettre à des étudiants japonais de poursuivre leurs études à l'étranger. Cette agence dispose d'un Centre de renseignement scientifique et technologique (le JICST). Les compagnies commerciales japonaises, qui emploient près de 60.000 personnes dans le monde, offrent également un cadre parfait pour le recueil d'informations, par le biais d'une infinité de contacts dans les pays où elles sont implantées. De très nombreuses entreprises disposent de leur propre système de collecte, extrêmement élaboré.

Au Japon aussi on note l'implication croissante des autorités régionales aux côtés des PME dans leurs initiatives d'intelligence économique ([119]).

Cette stratégie de renseignement scientifique et technologique est coordonnée au plus haut niveau avec le service de renseignement du premier ministre, le *Naichô*. L'Etat japonais et les entreprises fonctionnent donc en parfaite symbiose.

---

117 Voir : Richard Deacon , *Les extraordinaires réussites des services secrets japonais*, éditions Jacques Granger, Paris, 1986 ; Genovefa Etienne et Claude Moniquet, op. cit. volumes I et II.

118 DST, police secrète - Roger Faligot et Pascal Krop - Flammarion

119 Exemple : le site www.mydome.jp de Osaka Industrial Promotion Organization.

5.7. Les Etats-Unis d'Amérique.

Aux Etats-Unis, la philosophie libérale et un certain état d'esprit favorisant la libre entreprise ont facilité, dès le XIXème siècle, l'apparition de sociétés privées de renseignement et, comme au Japon mais pour des raisons différentes, une étroite imbrication des secteurs publics et privés. Ainsi, en pleine guerre de sécession, c'est à un détective privé, Allan Pinkerton, que l'armée du Nord fait appel pour organiser un service de renseignement militaire. Lorsqu'il se retirera, Pinkerton ([120]) créera la première agence de « police privée », toujours active de nos jours. Par la suite, les pratiques traditionnelles de la politique américaine (entre autres le traditionnel remplacement de centaines de hauts fonctionnaires à chaque changement de majorité) et la conception même de la vie publique voulant qu'il soit bien vu, dans certaines professions, de passer dix à vingt ans au service du gouvernement avant de se tourner vers des activités nettement plus lucratives, ont largement favorisé un large brassage entre secteur public et secteur privé. Ce brassage s'est étendu à la communauté du renseignement et a donné naissance à une industrie du renseignement privé et de la sécurité sans équivalent dans le monde occidental ([121]).

Aux Etats-Unis, le renseignement économique est en effet considéré comme une composante essentielle de la sécurité nationale, bénéficiant d'une priorité équivalente à celle du renseignement diplomatique, militaire et technologique.

L'approche américaine est beaucoup moins centralisatrice et beaucoup plus libérale que celle du Japon. Un des objectifs actuels de la politique générale des Etats-Unis est de défendre et de promouvoir leurs intérêts économiques, publics et privés, partout dans le monde, dans le cadre d'une société fondée sur l'accès ouvert à tous les marchés, la libre entreprise, la mondialisation et la déréglementation.

Le débat est longtemps demeuré vif aux Etats-Unis entre les tenants de la thèse voulant que les services de renseignement mettent leur moyen au service des entreprises, et ceux qui optent pour une position plus conforme avec les principes libéraux exigeant que les affaires de l'Etat ne soient pas confondues avec celles du secteur privé. Dans la première hypothèse, le principal problème réside dans la manière dont les services et les entreprises doivent coopérer afin de ne pas favoriser certains industriels aux dépens d'autres, et de ne pas fausser le jeu normal de l'économie de marché.

Le débat sur cette question est devenu un thème central de discussion sur le rôle des services secrets dés la fin de la guerre froide.

En avril 1992, le directeur de la CIA Robert Gates, s'exprimant devant la Chambre des représentants, affirmait clairement son opposition à la pratique de l'espionnage économique ou industriel ([122]). Cette attitude n'était cependant pas celle d'un de ses prédécesseurs, l'amiral Stanfield Turner, en poste de mars 1977 à janvier 1981 qui regrettait l'attitude timide de son service en cette matière : *"J'ai fait de gros efforts pour aider le monde américain des affaires; mais les professionnels de la CIA m'ont dit qu'il ne s'agissait pas là de dossiers intéressant la sécurité nationale"* ([123]).

---

120 Voir, les recherches du « *Center for Studies in Intelligence* » de la CIA sur les origines du renseignement américain.

121 Le monde anglo-saxon partageant la même culture du renseignement, on retrouve aussi en Grande Bretagne ce même brassage de personnel entre services de renseignement d'Etat et firmes privées.

122 Washington Post, 14 mars 1993, cité par Jean Guisnel "Guerre dans le cyberespace", 1995

123 Time Magazine, 28 mai 1990, cité par Jean Guisnel "Guerre dans le cyberespace", 1995

Parvenu à la présidence des Etats-Unis, Bill Clinton a considéré la consolidation des zones d'influence commerciales américaines traditionnelles, de même que la conquête de nouveaux marchés, comme l'une des priorités de son mandat en matière de politique étrangère. En 1993, il a offert l'appui de la communauté américaine du renseignement aux compagnies privées en créant le "*National Economic Council"* parallèlement au "*National Security Council*". Le 14 juillet 1995, Bill Clinton a félicité chaudement la CIA d'avoir su découvrir des cas de corruption qui auraient permis de soustraire des milliards de dollars de contrats à des entreprises américaines. "*Votre travail a contribué à la prospérité américaine*" a-t-il déclaré.

En 1994, le directeur de la CIA, James Woolsey déclarait : *"Nous n'espionnons pas au profit de firmes privées. Mais nous portons les cas de corruption pratiquée par des étrangers à la connaissance de la Maison Blanche, du Département d'Etat et du ministère du Commerce, qui ensuite tentent de redresser la barre, souvent avec succès".*

En 1997, un ancien directeur adjoint de la CIA, John Gannon, devenu président du "*National Intelligence Council*" a expliqué que les missions de renseignement économique sont de deux ordres :

- au plan stratégique, il s'agit d'alerter sur les tendances économiques internationales qui peuvent avoir un impact sur les intérêts américains; plus spécifiquement cela signifie anticiper les crises économiques, les menaces sur l'offre énergétique mondiale, évaluer les performances économiques de certains Etats, surveiller l'impact économique des sanctions internationales;
- au niveau tactique, il s'agit de fournir une information et une analyse sur les enjeux économiques importants aux responsables américains, en appui à leurs processus quotidiens de décision et à leurs interactions avec leurs homologues étrangers. Il convient notamment de "*s'assurer que tous les pays jouent avec les mêmes règles du jeu économique*".

Les officiels de la CIA pensent donc qu'ils ne doivent pas mener directement des actions contre des firmes étrangères pour le compte d'entreprises américaines, mais qu'ils doivent contenir l'espionnage économique clandestin à des domaines tels que les négociations commerciales, la protection des firmes nationales contre la pénétration par des agents secrets étrangers et la mise à jour de corruption rendant difficile la compétition dans des nations en développement ([124]).
Le livre de Jean Guisnel "Guerre dans le Cyberespace", paru en 1995, décrit pourtant quelques cas dans lesquels l'intervention des services de renseignement américains a sans doute permis à des firmes américaines de décrocher d'importants contrats internationaux. Parmi ceux-ci, on relève déjà les cas cités par Duncan Campbell dans son rapport présenté en février 2000 au Parlement européen sur le réseau "Echelon"([125]).

Les remous provoqués en 2000 par la parution de ce rapport ont d'ailleurs donné lieu à une nouvelle justification de la pratique du renseignement économique de la part des services de renseignement américains.

---

[124] Los Angeles Times, 15 juillet 1995 cité par Jean Guisnel dans "Guerres dans le Cyberespace", 1995

[125] Les cas des firmes "Panavia European Fighter Aircraft consortium", "Thomson CSF" et "Airbus industrie" sont cités dans le rapport *STOA "development of surveillance technology and risk of abuse of economic information - part 4/4"*

En effet, James Woolsey, n'étant plus alors directeur de la CIA, a confirmé que son service avait bien surveillé des firmes européennes en compétition avec des firmes américaines au cours d'importantes transactions internationales et ce, parce que les européens auraient eu recours à la corruption pour obtenir les marchés convoités ([126]). Seuls les gouvernements étrangers faisant l'objet de ces manœuvres auraient été avertis que les Américains ne le prenaient pas à la légère. Et M. Woolsey de critiquer l'interventionnisme des gouvernements européens qui soutiennent, souvent de manière déloyale, leurs entreprises plus coûteuses et moins performantes que les entreprises américaines : *"it is because your economic patron saint is still Jean Baptiste Colbert, whereas ours is Adam Smith"* lance-t-il à l'adresse des gouvernements européens. Si ceux-ci voulaient bien réformer leurs économies étatiques, pour les conduire à plus d'efficacité et d'innovation, ils ne devraient plus avoir recours à la corruption et les américains n'auraient plus besoin de les espionner, conclut M. Woolsey. Mais s'il admet que la CIA pratique le renseignement économique, il affirme aussi que 95 % des informations collectées proviennent de sources ouvertes. Il répète que son service n'est pas engagé dans des opérations d'espionnage économique au profit d'entreprises ou de sociétés américaines.

Le *Federal Bureau of Investigation* (c à d la police judiciaire fédérale) semble quant à lui jouer un rôle purement défensif en la matière. En 1998, un responsable de la sécurité nationale au FBI a affirmé lors d'une audition au congrès que les services de renseignement étrangers jouaient un rôle de premier plan dans l'espionnage industriel et économique au profit de leurs propres entreprises nationales, visant particulièrement les technologies de pointe, les brevets, mais aussi des informations confidentielles sur des contrats, des appels d'offre, des stratégies commerciales, etc. Le 13 septembre 2000, l' "*International Economic Policy and Trade Subcommittee"* de la Chambre des représentants a organisé une nouvelle série d'auditions afin d'évaluer les évolutions de l'espionnage économique contre les entreprises américaines. Des cabinets d'investigation et d'intelligence économique américains ont d'ailleurs tenté d'estimer les pertes occasionnées à l'économie américaine par l'espionnage économique : les estimations oscillent entre 42 et 200 millions $ par an.

Le FBI surveille donc de manière particulièrement attentive les firmes de communication étrangères qui cherchent à s'implanter aux Etats-Unis. Le FBI redoute en effet que ces opérateurs étrangers ne profitent de leur contrôle sur des réseaux américains pour mettre sur écoute des entreprises pour le compte des services de renseignement de leurs pays. De même, le FBI surveille les opérations de prise de contrôle d'entreprises américaines par des groupes étrangers dans le cadre d'une loi fédérale qui permet au président des Etats-Unis d'interdire toute acquisition "*pouvant affecter la sécurité nationale".*

Le *Economic Espionage Act* de 1996 permet au FBI et à d'autres agences fédérales de pratiquer des interceptions de communications à des fins de contre espionnage économique.

Il existe depuis 1977 un département de la NSA (*National Security Agency*) qui a pour mission de fournir des données au "*Departement of Commerce*" susceptibles d'être utilisées en vue de soutenir des intérêts économiques et commerciaux.

[126] Wall Street Journal, 7 mars 2000.

Le « *National Counterintelligence Executive (NCIX)* » a été créé par une directive présidentielle « *US Counterintelligence Effectiveness for the 21st Century* » de décembre 2000. Le NCIX coordonne et soutient les missions de contre-espionnage du gouvernement américain. Le NCIX a pour mission d'établir un dialogue entre l'administration et le secteur privé pour définir les informations, technologies et industries « critiques » dont la perte pourrait diminuer la puissance des Etats Unis. Cette agence est une expression de la nouvelle philosophie du gouvernement américain qui cherche à établir une coopération renforcée et une coordination entre les communautés du renseignement, du contre-espionnage et des forces de sécurité. Une des missions du NCIX est de sensibiliser les acteurs du secteur privé et public sur les menaces de l'espionnage économique. ([127])

Selon le Secrétaire d'Etat adjoint au Commerce du gouvernement américain, Samuel Bodman, la protection des systèmes d'informations stratégiques pour l'économie d'un pays est une composante essentielle de la « *homeland security* » ([128]) qui doit être assurée sous la responsabilité partagée des gouvernements et du secteur privé ([129]) entre lesquels la plus grande collaboration doit exister. Les projets de l'administration américaine en matière de sécurité de l'information devraient introduire la légalisation du métier de conseiller en sécurité informatique. Cette profession serait soumise à des obligations déontologiques comparables à celles des avocats ou des médecins.

Cette tendance se retrouve aussi largement dans les secteurs connexes du lobbying et des Sociétés Militaires Privées (ou *PMCs'*) auxquels ont désormais recours non seulement les compagnies multinationales, mais aussi certains gouvernements ([130]). Aux Etats-Unis ce secteur d'activités est soumis, comme le commerce des armes, à une seule et même législation, *the International Traffic in Arms Regulations (ITAR)*.

L'approche américaine des secrets économiques et commerciaux.

Aux Etats-Unis, l'information scientifique et technologique est très largement accessible au nom du libéralisme économique. Les événements qui secouèrent l'Amérique le 11 septembre 2001 ont cependant provoqué d'importantes restrictions dans l'accès aux informations d'ordre technologique. Mais l'espionnage économique et la manière de s'en prémunir sont des matières qui préoccupaient déjà le Congrès américain de manière intense bien avant 2001. En 1996, celui-ci a adopté l'*Economic Espionage Act (EEA)* qui tend à réprimer l'appropriation indue des *trade secrets* (les secrets commerciaux) aussi bien par des services de renseignement ou gouvernements étrangers que par des concurrents nationaux.

127 **www.ncix.gov**

128 *Homeland Security Act*, November 2002 - http://news.findlaw.com/wp/docs/terrorism/hsa2002.pdf

129 Allocution prononcée lors du « Forum pour la Sécurité de l'Information » tenu à Bruxelles le 28 octobre 2002, (http://www.uspolicy.be/Issues/Terrorism/bodman.102902.htm)

130 Voir point 6.7. ci-après.

Aux Etats-Unis, la manière de protéger les *trade secrets* diffère fondamentalement de la manière de protéger les secrets de la sécurité nationale. Ces derniers sont protégés par un rigoureux système de classification qui incrimine la possession même d'une information classifiée par une personne non habilitée, et ce, quelle que soit la manière dont elle a été acquise. La particularité de l'*Economic Espionage Act* est de ne pas incriminer la prise de connaissance d'un secret commercial en soi; c'est seulement la manière déloyale, trompeuse ou malhonnête utilisée pour prendre connaissance (ou tenter de prendre connaissance) d'un tel secret qui peut l'être. Pour qu'une information soit considérée comme telle, elle ne doit pas être répandue dans le domaine public, elle doit être la source d'une valeur économique pour son détenteur et celui-ci doit avoir pris des mesures raisonnables pour la garder secrète. Ceci n'empêche donc personne de tenter de percer ou de comprendre le secret d'un concurrent pourvu que les moyens employés soient honnêtes (par exemple, par l'analyse de sources ouvertes). Ce système de protection des secrets commerciaux repose donc sur la responsabilisation des acteurs économiques eux-mêmes ([131]).

5.8. Le Canada.

Le "*Service Canadien du Renseignement de Sécurité*" (SCRS) a créé une structure spécialisée dans le conseil de contre-espionnage au profit des entreprises. Dans son rapport d'activités de 1998, le Comité permanent R avait relevé la difficulté qu'éprouvait le SCRS à circonscrire sa mission dans le cadre d'une définition trop large de la notion de sécurité économique. Cette mission de sécurité économique se trouve décrite de manière plus précise dans une publication périodique éditée par ce service et intitulée "Série d'aperçus" (n 6 de mai 1998). Un des principaux objectifs du SCRS est de surveiller les activités menées au Canada par des officiers de renseignements étrangers, connus ou présumés, et d'empêcher des visiteurs, étudiants ou délégués étrangers soupçonnés d'activités de renseignement d'entrer au Canada. Le mandat du SCRS en matière d'espionnage économique est d'enquêter sur les activités clandestines de gouvernements étrangers qui sont susceptibles de nuire aux intérêts économiques et commerciaux du Canada. Le SCRS s'efforce de prévenir le gouvernement lorsque les règles du jeu équitables de la concurrence sur le marché libre sont délibérément infléchies contre le secteur industriel canadien.

Le SCRS ne s'intéresse pas à l'espionnage industriel, c'est-à-dire à l'espionnage exercé par une firme du secteur privé contre une autre. Lorsque ces activités sont de nature criminelle, ce sont les services de police qui enquêtent.
Le SCRS précise que l'espionnage économique n'est pas seulement le fait de gouvernements traditionnellement hostiles au Canada, mais qu'il existe des signes que certains pays considérés comme amis s'y livrent également ([132]).

---

131 *"OSINT - An American legal and practical perspective*" by Richard Horowitz, attorney at Law, EUFIS - Brussels 19 October 2000.

132 Le SCRS présente sa mission de protection de la sécurité économique du Canada sur son site http://www.csis-scrs.gc.ca/fra/operat/es2_f.html.

5.9. La Russie et les pays de la Communauté des Etats Indépendants.

En avril 1994, le président de la Fédération de Russie, M. Boris Eltsine a tenu un discours à l'intention des responsables et des collaborateurs des services de renseignement extérieur de son pays (SVR et GRU) dont l'extrait suivant est très clair au niveau des objectifs qui leur étaient assignés : *"Ce que nous attendons du Renseignement extérieur, ce sont des informations indispensables à l'adoption par l'Etat de décisions capitales touchant à la politique étrangère et intérieure de la Russie, à la mise en oeuvre de nos orientations économiques et du progrès scientifique et technique".*

Le rapport d'activités du service de renseignement allemand "*Bundesamt für verfassungsschutz*" (BfV) pour l'année 1999 donne quelques informations sur les activités de renseignement économique et scientifique auxquelles se livrent les services de renseignement russes, ukrainiens et bellarusses. Selon ce rapport, la collecte de renseignements d'ordre économique, scientifique et technique occupe à présent la première place dans les priorités de ces services.

Le SVR, service de renseignement extérieur russe, occupe environ 15.000 personnes. Selon son attaché de presse, ce service a reçu pour mission de créer à l'étranger des conditions favorables pour les intérêts économiques russes en vue d'attirer des investisseurs étrangers vers ce pays. Pour collecter leurs informations, les services de renseignement russes font usage aussi bien de sources ouvertes, que de moyens humains et techniques clandestins, tels que l'interception des communications. Comme sources ouvertes, ils utilisent la littérature, les bibliothèques, les banques de données, l'Internet, ils visitent des foires et missions commerciales, ils fréquentent des colloques et conférences et essayent d'y nouer des contacts intéressants. Pour le recueil clandestin de renseignements, les services russes utilisent des officiers de renseignements envoyés sous couvertures dans leurs ambassades et consulats, dans des agences de presse, dans des firmes d'Etat ou dont la majorité du capital est détenue pas des citoyens russes.

Toujours selon le BfV, le FSB (le service de renseignement intérieur) surveille à l'intérieur du pays les membres des ambassades et des postes consulaires étrangers, les hommes et femmes d'affaires venus en visite en Russie ainsi que les cadres et le personnel des firmes étrangères établies dans ce pays. Le rapport annuel du BfV pour l'année 2002 ([133]) confirme l'intense activité des services de renseignement russes en matière d'acquisition de connaissances technologiques utiles à leur industrie de l'armement.

Par ailleurs, la réforme des services de renseignement et les licenciements qui l'a accompagné ont jeté sur le pavé nombre d'incontestables talents de ces services.
Dans le même temps, l'essor de l'économie privée, l'implantation de nombreuses sociétés étrangères et l'explosion de la criminalité ont créé un double besoin jusque là inconnu dans le pays: celui de l'obtention rapide d'une information économique précise par les nouveaux décideurs privés mais aussi d'une protection contre les rackets et les agressions de la mafia. Cette évolution parallèle (disponibilité de bons spécialistes et apparition d'une forte demande dans leur secteur) ne pouvait qu'être à l'origine d'une floraison de sociétés de sécurité privées. ([134]).

[133] Verfassungsschutzbericht 2002, pp. 223, 237 et 238.
[134] Genovefa Etienne et Claude Moniquet, op.cit., vol. II.

Aujourd'hui, ces firmes privées de renseignement russes peuvent s'appuyer sur la théorie du «*deuxième mur de la sécurité nationale* ». L'état russe n'ayant plus la possibilité de remplir toutes les missions de sécurité qui sont les siennes, il s'en remet pour partie à des services privés, sous son contrôle, qui en contrepartie profitent des relations ainsi établies pour défendre les intérêts de leurs clients. Les plus importantes des sociétés ont d'ailleurs été regroupées au sein d'un conseil consultatif qui entoure, pour certaines matières, la direction des services de renseignement d'Etat. Or, nombre de ces sociétés entretiennent des liens très étroits avec des sociétés amies en Europe centrale ou y créent des filiales.

5.10. Autres pays (en bref)

Quelques revues et ouvrages spécialisés évoquent aussi la place du renseignement scientifique et économique dans des pays comme :

- **La Chine populaire :** l'Académie des sciences chinoise offre chaque année des bourses à de nombreux professeurs d'universités, responsables de laboratoires et chefs de recherches de pays étrangers pour qu'ils s'associent à des plans de recherches chinois. ([135]). La section renseignement et contre espionnage économique et financier du ministère de la sécurité chinoise ("Guoanbu") a notamment reçu pour mission d'empêcher les étrangers de se procurer l'information économique qui n'a pas été préalablement triée par les autorités. Ce tri est effectué conjointement par le Guoanbu, le ministère du commerce extérieur et de la coopération économique et le département de propagande du Comité central du parti communiste chinois. ([136]).
- **La Chine nationaliste** est, elle aussi, considérée comme l'un des pays les plus efficaces en renseignement économique. ([137]).
- **La Suède :** plusieurs entreprises suédoises pratiquent l'Intelligence économique en toute discrétion depuis le début du siècle. Ceci peut expliquer leurs succès commerciaux dans le monde. L'université de Lund s'est spécialisée dans cette matière.
- **Israël :** selon les experts du Comité, le marché de la sécurité privée est, par la force des choses, une industrie florissante en Israël ou pour des ressortissants israéliens vivant et travaillant à l'étranger. Bénéficiant d'une excellente formation, retraités très jeunes (entre 40 et 45 ans s'ils le souhaitent) les militaires et agents de renseignement israéliens sont très demandés. Nombre d'entre eux ont créé des sociétés ou des cabinets de conseil. Une grande partie de ces entreprises se spécialisent dans la protection physique et la sécurité des lignes aériennes et des installations aéroportuaires ou encore la sécurité des réseaux informatiques, mais d'autres se livrent au renseignement privé pur.

135 "*Le Monde du Renseignement*" (LMR) n° 338 02/07/1998
136 LMR n° 304 30/01/1997
137 LMR n° 356 08/04/1999

5.11. Conclusions.

La manière de recueillir et de protéger le renseignement d'ordre scientifique et économique s'est développée de manière extrêmement variée suivant les pays. La place du marché du renseignement privé y est très mouvante et particulièrement complexe à appréhender : les sociétés de renseignement privé naissent et disparaissent rapidement, d'autres ne sont que de simples boîtes aux lettres. Ces différences induisent aujourd'hui des niveaux d'efficacité (ou de dangerosité selon l'appréciation) ainsi que des pratiques professionnelles très différentes suivant que l'on parle d'opérateurs japonais, américains, français, russes ou israéliens pour se limiter aux quelques exemples qui ont été ici brièvement abordés.

6. L'ETAT DU MARCHE DU RENSEIGNEMENT PRIVE EN BELGIQUE.

L'Annuaire européen des Professionnels de l'Intelligence Economique édité en France par la Société d'Intelligence Economique et Concurrentielle appliquée" (SIECA) recensait déjà en 1998 plus de trente sociétés actives en matière d'intelligence économique et de renseignement privé en Europe. En 2003, l'ouvrage *« France : le top 100 de l'intelligence économique »* recense plus de 100 prestataires reconnus ainsi que les structures existant au sein de grandes entreprises, d'organismes publics ou parapublics ([138]). Parmi eux, une moitié seulement développent une communication volontaire et ouverte sur leurs activités.

Le marché belge est encore relativement vierge en matière de veille et d'intelligence économique, contrairement aux Etats-Unis ou à la France. Pourtant, sa situation géographique et la concentration d'institutions internationales d'envergure (Union européenne, OTAN, UEO, etc.) sur son territoire confèrent à la Belgique, et à Bruxelles en particulier, une importance politique et stratégique non négligeable. La Belgique est donc une terre d'accueil pour des entreprises multinationales, les cabinets de lobbying et les marchands d'informations. Les institutions européennes constituent elles-mêmes une source d'informations très importante.

L'ouvrage « *Kwestbare Kennis* » de Marc Cools et Bob Hoogenboom rapporte les propos d'un ancien collaborateur d'une firme américaine de renseignement qui désigne la Belgique comme « *le Walhalla des courtiers en informations* ». Il déclare notamment : « *Bruxelles est un centre d'affaires international pour les multinationales qui veulent s'établir dans la capitale de l'Union européenne. Les institutions européennes sont elles-mêmes une source importante de renseignements. Je pense que ces institutions ne sont pas suffisamment protégées. C'est un circuit bavard qui fuit de tous les côtés. La plupart des fonctionnaires européens n'ont aucune notion des règles de sécurité les plus élémentaires. Bruxelles est un cauchemar pour les gens de la sécurité mais un rêve pour les curieux. »* (Traduction libre).

[138] *« France : le top 100 de l'intelligence économique Intelligence On Line reports » Editions Indigo Publications, Paris 2004*

6.1. Les cabinets d'audit.

Quatre grands cabinets d'audit (les *big four*) sont présents en Belgique. Ici comme ailleurs dans le monde, des juges d'instructions, des officiers du ministère public font de plus en plus souvent appel à des consultants issus de ces cabinets d'audit pour être désignés comme experts dans des affaires pénales ou de fraudes fiscales en rapport avec le monde des affaires. La commission d'enquête parlementaire chargée d'examiner les causes de la faillite de la SABENA a elle-même fait appel à ces consultants privés. Ces 4 derniers grands cabinets d'audit d'envergure internationale offrent dans notre pays leurs compétences en matières d'audit de fraudes en entreprises (*Forensic Services*) mais on ne retrouve pas dans les organigrammes de leurs filiales belges de département d'intelligence ou de renseignement économique. Les experts du Comité notent que ces big four ont en effet choisi de rester très discrets sur ce genre d'activité. Selon eux, cette situation est sans doute générée par les spécificités du marché belge dans ce domaine, mais qui ne reflète pas la position de ces groupes dans les pays anglo-saxons par exemple, dans lesquels des filiales très offensives, comprenant du personnel provenant bien souvent des services de renseignement, se développent sur des marchés demandeurs de ce type de services.
Dans son rapport intitulé « *Intelligence économique, compétitivité et cohésion sociale* », le député français Bernard Carayon ([139]) souligne que dans les pays anglo-saxons, des services de renseignement sont étroitement imbriqués avec des entreprises « *qui ont pour métier de conseiller, d'auditer, d'assurer, d'investir et d'innover* ».

Pour des questions légales et d'images, les experts du Comité permanent R estiment impossible que lesdits cabinets développent, en Belgique, des activités de renseignement. Toutefois les experts n'excluent pas que, saisi d'une telle demande par un client étranger, les sièges anglo-saxons de ces cabinets pourraient peut-être agir en mettant en application la méthode des « coupe-circuits ».

6.2. Firmes, agences, officines et autres cabinets étrangers offrant des services de renseignement privé ou disposant d'une représentation en Belgique ou y exerçant des activités depuis l'étranger.

Les experts du Comité ont dénombré une quinzaine de petites ou moyennes agences françaises susceptibles de développer leurs activités en Belgique. Il s'agit d'agences de faibles dimensions en comparaison des multinationales américaines. Elles sont souvent fondées ou dirigées par d'anciens militaires, fonctionnaires de police ou membres des services de renseignement français.

Les experts n'ont pas connaissance, à ce jour, d'activités particulières de sociétés allemandes de renseignement privé sur le sol belge. L'Allemagne étant historiquement tournée vers l'Est, c'est sans doute en Europe centrale et en Russie qu'on doit trouver des têtes de pont du renseignement privé allemand. Les experts pensent toutefois que cet état de fait pourrait changer. Selon eux, la crise économique que traverse l'Allemagne est telle que ses entreprises devraient se montrer de plus en plus agressives.

[139] Voir point 5.2.3.

Les experts indiquent quelques sociétés britanniques et américaines présentes ou actives sur le sol belge, mais ils pensent que la plus grande partie du renseignement « privé » américain en Belgique passe par d'autres canaux comme les chambres de commerce, certaines multinationales qui disposent souvent de services internes spécialisés ou encore des cabinets d'avocats qui ont pour mission de « s'intéresser » de très près aux entreprises européennes, à leur faiblesse ainsi qu'aux aides que leur apporte l'Union européenne.

Les experts notent que le marché de la sécurité privée est une industrie florissante en Israël ou pour des ressortissants israéliens vivant et travaillant à l'étranger. Il existe des firmes privées israéliennes spécialisées dans la protection physique et la sécurité des lignes aériennes, des installations aéroportuaires ou encore dans la sécurité des réseaux informatiques, tandis que d'autres se livrent au renseignement privé pur. Les experts ne citent que deux sociétés israéliennes de renseignement privé susceptibles de développer des activités en Belgique. Le Comité permanent R note pour sa part que la police fédérale belge se fournit auprès d'une firme israélienne spécialisée dans la mise au point et la fourniture de matériels électroniques de haute technologie, destinés à intercepter des communications téléphoniques.

On verra aussi plus loin ([140]) que le Japon a développé un système global de collecte d'informations dans lequel chacun, du simple citoyen (et, a fortiori, de l'employé de base) jusqu'aux responsables gouvernementaux, est susceptible de collecter des renseignements. Les experts mentionnent quelques associations professionnelles et organismes publics ou semi-publics japonais représentés à Bruxelles susceptibles de collecter des informations d'ordre scientifique et économique. Les experts notent également qu'une secte d'origine japonaise épinglée dans l'enquête parlementaire de 1997, est régulièrement soupçonnée de se livrer à l'espionnage économique. Cette secte qui chercherait à pénétrer tous les centres de pouvoir et de décision est officiellement présente en Belgique.

Les experts attirent l'attention du Comité permanent R sur les risques que font courir à l'Union européenne, donc aussi à la Belgique, l'élargissement programmé de l'Union Européenne. Demain, plusieurs pays d'Europe centrale intégreront l'Europe. Leurs sociétés commerciales auront donc un accès immédiat et total au marché européen. Parmi ces sociétés, figurent des entreprises de sécurité et de renseignement privé qui entretiennent des liens très étroits avec des sociétés proches des services de renseignement russes ou en sont même les filiales. Le risque existe donc de les voir servir de couverture pour des activités de collecte de renseignement au profit des services russes.

6.3. Officines et sociétés belges

A l'inverse de ce qu'ils constatent dans les pays voisins, les experts ne dénombrent que très peu de firmes, agences, officines ou services d'intelligence économique ou de renseignement belges. « *En raison des facteurs stratégiques et sensibles auxquels la veille et l'intelligence économique touchent, les entreprises belges rechignent encore à faire appel à une aide extérieure « professionnelle » pour les assister dans ces missions. La méconnaissance de la discipline et des outils, d'une part, la faiblesse de l'offre, d'autre part, renforcent cette attitude. Ajoutons à cela la difficulté de chiffrer l'éventuel « retour sur investissement » que représente une telle approche qui tient plutôt de l'assurance que du placement.* » Il est vrai que la veille stratégique est un processus à faible rendement immédiat alors que les attentes des entreprises sont à court terme.

[140] Voir point 5.5.

Quelques petites entreprises belges proposent toutefois des services d'analyses et d'audits de sécurité en entreprises, de gestion de l'Information, de veille technologique, d'Intelligence économique et stratégique, de contre-intelligence, de biométrie, de courtage en information, ainsi que des séminaires de formation aux métiers de l'intelligence économique. Quelques bureaux belges de détectives annoncent qu'ils effectuent des missions relevant du renseignement économique privé.

6.4. Sociétés établies en Belgique et possédant une cellule ou un service de renseignement interne

Peu d'entreprises belges sont dans ce cas. Les experts expliquent cet état de chose par trois facteurs typiques de notre pays :

- les investissements nécessaires à la mise en place de telles structures (ressources humaines et matérielles) sont importants et ne peuvent être assumés que par des sociétés ayant déjà atteint une certaine taille;
- la plupart des sociétés répondant à ce critère et implantées en Belgique ont leur centre de décision (et donc le principal bénéficiaire de ce genre de service), à l'étranger;
- les efforts de sensibilisation, de formation et d'aide en ces matières restent relativement discrets.

Cependant, les experts notent que les grandes entreprises ou les grands groupes internationaux présents sur différents marchés et continents disposent tous de ce type de cellule, généralement localisée dans les bureaux de la maison-mère. Les experts considèrent que les 500 ou 1000 - premières sociétés américaines (Fortune 500) disposent en leur sein d'un service ou - au minimum - d'une cellule d'intelligence ou de renseignement économique.

Les secteurs les plus demandeurs de ce type de disciplines sont les opérateurs de télécommunications, les industries pharmaceutiques, de l'armement, de l'aérospatiale, des hautes technologies, de l'agroalimentaire, les secteurs pétrolier et chimique, etc.

Les entreprises qui disposent en Belgique d'une fonction, d'une cellule ou d'un service de veille ou d'intelligence économique, se retrouvent dans les secteurs des télécommunications, de la haute technologie, de l'industrie chimique, de l'armement, de l'aéronautique et de l'espace.

Les experts notent que les renseignements disponibles sur les structures existantes, leur mode de travail et l'organisation sont limités, sans doute en raison d'une volonté affichée de maintenir une certaine discrétion sur des activités très souvent assimilées à de l'espionnage économique.

D'autre part, si de nombreuses entreprises revendiquent de pratiquer la veille ou l'intelligence économique, les experts estiment que cela se résume très souvent à des études de marché ou à une gestion documentaire plus ou moins élaborée. Selon eux, rares sont celles qui disposent réellement de compétences et d'outils adaptés. Certaines sociétés de type scientifique ou technologique parlent de "*scouting*", approche que l'on peut relier à la veille technologique.

6.5. Un nouveau rôle pour les associations professionnelles

Même si elles ne peuvent offrir qu'un service limité en cette matière, on constate que des associations professionnelles, sectorielles ou régionales, commencent également à promouvoir parmi leurs affiliés la pratique de la veille technologique et concurrentielle.

Ces initiatives bénéficient du soutien financier de la Région wallonne et du Fonds Européen de Développement Régional (FEDER) de l'Union européenne. Partant du postulat que de nouveaux métiers liés à la gestion de l'information sont en train de se créer, ces deux associations aident les entrepreneurs et les PME de leurs régions à se familiariser à la gestion de l'information stratégique. Seule ou en partenariat avec des professionnels, ces associations proposent des formations, des conseils et des services en matière de veille informative, normative, concurrentielle, partenariale et technologique, etc.

6.6. Associations non commerciales ayant pour objet social la pratique, l'étude et la promotion du renseignement.

Le Comité permanent R note enfin l'apparition récente en Belgique de plusieurs associations sans but lucratif ayant pour objet social l'étude du renseignement et des menaces de sécurité ainsi que la promotion de la « culture du renseignement et de la sécurité».

Ces asbl organisent des échanges, des conférences, des séminaires et des études scientifiques, destinés aux professionnels du renseignement à qui elle propose aussi des services d'expertise.

Ces associations sont composées de hauts fonctionnaires, de professeurs d'universités d'anciens journalistes, de consultants et de juristes, tous spécialisés dans le domaine du renseignement.

6.7. L'enseignement de la veille et de l'intelligence économique en Belgique.

Ces matières trouvent encore très peu d'écho dans les universités et écoles supérieures en Belgique. Quelques initiatives méritent cependant d'être signalées dans l'enseignement de la Communauté française, l'une à l'Université Libre de Bruxelles, l'autre à l'Université de Mons ainsi que deux *Master of Business Administration (MBA)* en cours du soir.

L'enseignement de l'intelligence économique à l'université libre de Bruxelles (ULB) : *l'enseignement de cette matière y est approché sous la forme de deux cours dans la formation INFODOC, accessibles uniquement après une candidature : « veille technologique » et « aide à la décision et traitement de l'information ».*

Le diplôme européen en intelligence économique et stratégique (DEIES) de l'université de Mons ([141]) : ayant constaté l'absence d'enseignement en cette matière au nord de Paris, l'Université de Mons – Hainaut et l'Ecole Supérieure des Affaires de l'Université de Lille 2 se sont associées au cours de l'année académique 2002 / 2003 pour créer une formation menant à la délivrance d'un diplôme européen en intelligence économique et stratégique (DEIES). Il s'agit d'une formation de troisième cycle, limitée en volume horaire (150 heures réparties sur six mois) et accessible aux étudiants des diverses universités européennes déjà nantis d'une maîtrise (quatrième année d'université) ainsi qu'aux cadres d'entreprises, d'organisations territoriales, d'associations ou d'ONG ayant au moins cinq ans d'expérience. Cette formation porte sur les outils de veille juridique, technologique, commerciale, sur les méthodes d'analyses des dangers qui guettent les entreprises et les organisations et les moyens utilisés pour s'en protéger.
L'association entre les universités de Mons et de Lille II pour ce programme d'enseignement n'a, en effet, pas été renouvelée.

The Master of Business Administration (MBA) of The United Business Institute ([142]) : The United Business Institutes à Bruxelles propose un Master of Business Administration (MBA en une ou deux années de cours du soir dans des matières telles que la « Corporate Intelligence & Knowledge Management » ou « Lobbying & Business Representation ».

La « Business Intelligence » est une matière également enseignée dans le cadre d'un MBA organisé par la **Solvay Business School** : ([143]). Cette formation ne s'adresse qu'à des titulaires de diplômes commerciaux ayant déjà une expérience professionnelle de deux ou trois ans ; les prix de la formation sont également très élevés (20.000 à 30.000 €).

Le Comité permanent R n'a connaissance d'aucun enseignement d'une telle nature dans la Communauté flamande du pays.

Par ailleurs, les réformes lancées depuis 1999 visant à harmoniser l'enseignement supérieur et universitaire au niveau européen, conjuguées à la faiblesse du financement public en Communauté française, laissent planer beaucoup d'incertitude sur l'avenir de l'enseignement de l'intelligence économique en Belgique.

Par ailleurs, il semble que les jeunes diplômés issus de ces formations spécialisées en Intelligence économique éprouvent des difficultés à être engagés comme tels. Les entreprises et les cabinets leur préféreraient en effet des seniors disposant d'une expérience professionnelle plus classique.

6.8. Offres de prestation de Sociétés Militaires Privées (SMP) en Belgique.

Les experts du Comité permanent R n'ont connaissance d'aucune SMP active en tant que telle en Belgique. Ils signalent toutefois que certaines sociétés de renseignement privé présentes en Belgique ont également des activités de SMP.

141 www2.univ-lille2.fr/esa/presentation/formation/DEIES.pdf
142 www.ubi.edu
143 *http://solvay.ulb.ac.be/mba/mba_bi.html*

6.9. Le renseignement spatial privé en Belgique.

Le Comité permanent R relève l'existence d'une spin-off ([144]) spécialisée dans l'interprétation d'images satellitaires.

Cette jeune entreprise se décrit comme un service multi-sectoriel d'information géographique satellitaire privilégiant les missions à caractère humanitaire et les activités de développement durable en Afrique centrale. Les clients de cette société sont des sociétés minières, des organisations humanitaires et l'Union Européenne (dans le cadre de son programme de gestion des zones de santé en RDC ou du projet ISIS). Cette firme a ainsi établi la cartographie géologique et routière de certaines régions d'Afrique et d'Asie en vue de permettre à des organisations humanitaires de préparer leurs interventions sur le terrain.

7. QUELS MOYENS L'ARSENAL LÉGISLATIF BELGE PERMET-IL DE METTRE EN ŒUVRE AFIN DE PROTÉGER LES SECRETS ÉCONOMIQUES, SCIENTIFIQUES ET TECHNOLOGIQUES DU PAYS ?

En Belgique, ces secrets ne sont protégés que de manière périphérique et non pas en tant que tels. Contrairement à la France, ils ne figurent pas parmi les secrets qui intéressent les intérêts fondamentaux de la nation comme la défense du territoire ou la sûreté de l'Etat dont la protection est organisée par un certain nombre de dispositions figurant au chapitre II du titre Ier du livre II du code pénal (intitulé *"crimes et délits contre la sûreté extérieure de l'Etat"*). Ils sont pris en considération par certaines lois particulières dans la mesure où ils intéressent des intérêts d'ordre plus généraux du pays.

7.1. La loi du 10 janvier 1955 "relative à la divulgation et à la mise en oeuvre des inventions et des secrets de fabrique intéressant la défense du territoire ou la sûreté de l'Etat".

Aux termes de cette loi, la divulgation volontaire ou par négligence de ces inventions et secrets de fabrique est passible de sanctions pénales. Il faut cependant prouver que l'auteur de la divulgation ne pouvait ignorer qu'elle était contraire aux intérêts de la défense du territoire ou de la sûreté de l'Etat. A cet égard, le ministre qui a la propriété industrielle dans ses attributions (le ministre des Affaires économiques) et le ministre de la Défense nationale peuvent déclarer conjointement que la divulgation d'une invention ou d'un secret de fabrique est contraire aux intérêts de la défense du territoire ou la sûreté de l'Etat et qu'elle est interdite pendant la période qu'ils déterminent.

[144] Une spin-off est une entreprise créée dans le sillage d'une université ou d'un centre de recherche scientifique dont elle exploite commercialement les applications scientifiques qui y ont été mises au point.

Les deux ministres précités, agissant conjointement, peuvent également déterminer et contrôler temporairement les conditions d'exploitation, d'invention et de mise en oeuvre de certains brevets qu'ils estiment devoir maintenir secrets; ils peuvent même en interdire temporairement leur exploitation ou leur mise en oeuvre, ou bien encore réserver à l'Etat, et à lui seul, le droit de les exploiter en tout ou en partie. Ces mesures peuvent être levées à tout moment, partiellement ou totalement, par décision des ministres dont elles émanent. Le titulaire du droit sujet à interdiction ou limitation peut solliciter cette mainlevée. Des sanctions pénales sont aussi prévues pour les infractions à ces mesures.

La loi de 1955 fixe une procédure par laquelle le ministre des Affaires économiques soumet une demande de brevet au ministre de la Défense nationale en vue de la mise en oeuvre des mesures précitées. Cette loi prévoit encore que *"lorsque, dans l'intérêt de sa défense, un Etat étranger interdit la divulgation d'une invention, objet d'une demande de brevet, le ministre ayant la propriété industrielle dans ses attributions s'abstiendra, sur requête de cet Etat ou du déposant qui établira la preuve de l'interdiction, de la communiquer au public et de délivrer des copies de sa description, aussi longtemps que durera cette interdiction".* Une telle requête ne peut toutefois être prise en considération que s'il existe une convention entre la Belgique et l'Etat étranger auteur de l'interdiction

Jusqu'au vote de la loi du 11 décembre 1998 *"relative à la classification et aux habilitations de sécurité"*, la loi de 1955 était la seule en droit belge qui attribuait à une autorité politique la responsabilité de décréter le secret d'informations à caractère économique.
Entre 1949 et 1994, la Belgique a participé à la concertation COCOM (*Coordinating COMmittee*) des pays occidentaux regroupés à l'instigation des Etats-Unis en vue d'exercer un embargo sur les exportations d'une série de produits et de technologies militaires, nucléaires mais aussi, et surtout, civiles à double usage (civil et militaire) à destination de l'URSS, de la Chine et des autres pays communistes. A ce titre, la Belgique a publié et tenu à jour pendant environ quarante ans une liste commune établie par le COCOM de produits et technologies soumis à contrôle, sous la forme d'un *"avis aux importateurs et exportateurs relatif aux produits et technologies soumis au contrôle de la destination finale".* Par ailleurs, la Belgique participe à différentes initiatives internationales destinées à limiter la prolifération de certaines technologies et armes de destruction massive. L'ensemble de ces produits et technologies contrôlés est regroupé au sein d'une liste unique de contrôle des produits et technologies à double usage mise au point par les Etats membres de l'Union européenne ([145]).

Cette réglementation européenne assure un contrôle harmonisé sur les exportations extra-communautaires tout en permettant la libre circulation au sein de l'Union de la quasi-totalité des produits et technologies à double usage. A cette réglementation européenne, il faut ajouter l'Arrangement de Wassenaar du 19 décembre 1995, entré en vigueur en juillet 1996, qui regroupe trente-trois Etats, parmi lesquels les pays de l'ancien COCOM et certains autres pays industrialisés ou anciens membres du bloc de l'Est, comme la Russie, la Hongrie, la Pologne, la Slovaquie et la République tchèque. Chacun de ces pays s'est engagé à ne pas autoriser l'exportation de biens ou technologies civiles à double usage ainsi que des matériels de guerre vers des pays dont *"le comportement irresponsable menace la paix et la sécurité internationale" (roge states).*

Il faut encore souligner que le premier but de ces conventions internationales n'est pas la protection du potentiel scientifique ou économique en soi. Elles ont été conçues plus en vue du maintien de la stabilité mondiale et de la non prolifération des armes de destruction massive que de la simple sécurité nationale. C'est la raison pour laquelle certains produits figurant sur ces listes n'ont aucune valeur de haute technologie.

---

[145] Règlement CE n° 3381/94 du Conseil, du 19/12/1994 instituant un régime communautaire de contrôle des exportations de biens à double usage.

7.2. La loi du 11 avril 1994 relative à la publicité de l'administration.

La protection des intérêts économiques est prise en compte dans les articles 4 et 5 de cette loi qui institue et organise le droit des particuliers de prendre connaissance d'un document administratif ou d'un document à caractère personnel d'une autorité administrative fédérale, de le consulter sur place, d'obtenir des explications à son sujet et d'en recevoir une copie. La demande de consultation doit cependant être rejetée lorsque l'intérêt de la publicité ne l'emporte pas sur la protection de certains intérêts collectifs parmi lesquels figurent *"un intérêt économique ou financier fédéral, la monnaie, le crédit public"* ainsi que "*le caractère par nature confidentiel des informations d'entreprises ou de fabrication communiquées à l'autorité"*.

7.3. La loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité.

Depuis l'adoption de cette loi, toute information, tout document ou données, matériel, matériaux ou matière, sous quelque forme que ce soit, dont l'utilisation inappropriée peut porter atteinte (gravement ou très gravement) au potentiel scientifique et économique du pays peut désormais faire l'objet d'une classification confidentiel, secret ou très secret (selon la gravité présumée de l'atteinte).

La diversification et l'hétérogénéité croissante des acteurs du secret (cfr 4.2.3. ci-avant) a donc été partiellement prise en compte par la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité puisque l'autorité compétente peut imposer la possession d'une habilitation de sécurité à des personnes morales ou physiques pour la passation et l'exécution de certains contrats ou marchés publics en rapport avec la Défense nationale, l'énergie nucléaire et la sécurité (article 12 alinéa 1). L'alinéa 2 du même article dispose : *"Dans les cas déterminés par le Roi, la présente loi s'applique également aux habilitations de sécurité demandées par des personnes morales ou physiques qui souhaitent obtenir une habilitation de sécurité en vue d'accéder à l'étranger à des informations, documents ou données, à des matériels, matériaux ou matières classifiées, à des locaux, des bâtiments ou des sites, dont l'accès est réservé au titulaire d'une habilitation de sécurité".* A cet effet, les entreprises titulaires d'une habilitation de sécurité doivent désigner un membre de leur personnel, lui-même titulaire d'une habilitation de sécurité, pour remplir la fonction d' "*officier de sécurité".* Cette fonction consiste à veiller à l'observation des règles de sécurité dans l'entreprise.

Le titulaire d'une habilitation de sécurité qui, dans l'exercice de ses fonctions, utilise ou laisse utiliser *"de manière inappropriée"* des documents, informations ou matériels classifiés est passible de sanctions pénales. Cette infraction est sanctionnée qu'elle ait été commise de manière délibérée, ou par négligence grave ([146]).

[146] article 11 de la loi du 11 décembre 1998 *relative à la classification et aux habilitations de sécurité*.

8. LES ATTENTES ET LES PROPOSITIONS DES MILIEUX ECONOMIQUES BELGES.

En 1986, peu après les attentats des CCC, un groupe de travail de la Fédération des entreprises de Belgique (FEB) s'est mis en place pour édicter des lignes directrices de sécurité aux chefs d'entreprises. En 1994, des experts en sécurité de divers secteurs industriels et d'entreprises ont créé une "*Plate-forme de concertation permanente pour la protection des entreprises"* (PCPE). Les secteurs les plus concernés étaient notamment la distribution, l'alimentation, la chimie, Fabrimetal, Sabena, Belgacom, le secteur pétrolier, les banques, les assurances, le secteur sidérurgique et l'industrie du tabac. Les experts en sécurité de ces secteurs se sont penchés sur tous les aspects de la protection des entreprises contre les risques d'origine criminelle. Des contacts ont été établis avec les autorités publiques et leurs services compétents, notamment la Sûreté de l'Etat et le SGR. En 1995, la PCPE a adressé à ces autorités un mémorandum exprimant les attentes et les propositions des milieux industriels belges en matière de sécurité des entreprises. Ce document a été réactualisé en juin 2000. L'espionnage économique y apparaît comme l'une des préoccupations majeures de la FEB parmi lesquelles on trouve aussi les attaques armées, les vols, les agressions violentes et les attentats. La FEB appelle donc à une redynamisation de la concertation entre pouvoirs publics et secteur privé, elle plaide pour une "*gestion intégrale de la sécurité*" et formule des propositions, parmi lesquelles deux concernent directement les services de renseignement :

- la création au sein du ministère de la Justice d'une structure permanente de contact avec le secteur privé : "Cette structure, composées de représentants des services de police, des services de renseignement et de la magistrature, devrait informer régulièrement la FEB, quant aux menaces pesant sur les entreprises et définir les projets de coopération entre le public et le privé". L'objectif est ici d'analyser en permanence les formes de criminalité qui constituent une menace contre les entreprises.
- "l'organisation de cours et cycles de formation pour le personnel dirigeant des services de police, des services de renseignement et de la magistrature, consacrés à l'organisation de l'entreprise et aux formes de criminalité dont les entreprises sont victimes." Pour la FEB, le personnel de ces services manque en effet d'expertise dans les domaines de la criminalité touchant les entreprises; il doit donc pouvoir disposer d'une formation adéquate axée sur la réalité des entreprises. "Il s'indique, par ailleurs, de mettre des "techniciens" à la disposition des services de police et/ou des parquets pour des enquêtes spécifiques visant le potentiel technologique et économique de notre pays".

Quatre groupes de travail furent mis en place au sein de la PCPE : «criminalité violente et hold-up », « criminalité économique », « formation » et « recherche ». La Sûreté de l'Etat se fit seulement représenter au sein du groupe « criminalité économique ». C'est dans ce cadre que le 18 février 1997, un directeur et un conseiller de ce service ont donné à des responsables d'entreprises une conférence de sensibilisation sur « *les sectes nuisibles dans leurs rapports avec le monde des affaires ».* Dans son plan de sécurité de juin 2000, le gouvernement fédéral déclare que les ministres de la Justice et de l'Intérieur poursuivront la concertation mise en place au sein de la PCPE et qu'un groupe de travail mixte chargé de la criminalité économique devra prêter attention aux modes criminels suivants : criminalité informatique, blanchiment d'argent, corruption et espionnage économique.

9. LES ACTIVITES MENEES PAR LES SERVICES DE RENSEIGNEMENT BELGES DANS LE CADRE DE LA PROTECTION DU POTENTIEL SCIENTIFIQUE ET ECONOMIQUE ?

9.1. La Sûreté de l'Etat.

9.1.1. Le contre-espionnage classique.

Jusqu'à la loi du 30 novembre 1998, la protection du patrimoine scientifique et économique du pays ne figurait pas comme telle parmi les sujets de préoccupation de la Sûreté de l'Etat.

Dans les années 70 et 80, en pleine guerre froide, les activités de la Sûreté de l'Etat en matière de protection du potentiel scientifique et économique se situaient principalement dans le cadre du contre-espionnage. Les services de renseignements des pays de l'ancien bloc communiste étaient très actifs en Belgique dans le recueil d'informations à caractère scientifique et technologique ([147]). Dans ce cadre, des entreprises belgo-soviétiques implantées dans la région d'Anvers ou dans les environs d'autres installations portuaires attiraient alors l'attention de la Sûreté de l'Etat. Il s'agissait d'y détecter d'éventuelles activités d'espionnage ainsi que les pressions occultes que des entreprises soviétiques ou satellites étaient susceptibles d'exercer sur des entreprises belges à l'occasion de certains contrats. Des contacts furent établis avec de nombreuses firmes belges afin de les briefer sur les risques encourus lors de telles relations. Le résultat de cette activité de contre-espionnage fut la découverte d'espions venant de l'Est et leur renvoi dans leurs pays d'origine. La Sûreté de l'Etat recueillait et analysait aussi des renseignements en vue d'empêcher l'exportation de matériel ou le transfert de technologies sensibles à destination de pays jugés « à risques », d'organisations maffieuses ou terroristes. C'est aussi dans ce cadre que la Sûreté de l'Etat a établi ses premiers contacts avec des firmes commerciales, des universités et des centres de recherche. L'attention du service a été attirée par les activités suspectes de certains hommes d'affaires, stagiaires ou étudiants étrangers.

Après l'effondrement de l'empire soviétique, la chute du mur de Berlin et la dissolution du pacte de Varsovie, les traditionnelles activités d'espionnage des pays de l'Est à l'égard de l'Occident semblèrent avoir cessé. Pourtant la Belgique procéda encore en 1992 à l'expulsion de quatre ressortissants russes convaincus d'avoir maintenu actif dans le pays un réseau de recueil de renseignements d'ordre scientifique et technologique.

En 1994, le président Boris Ieltsine confirma la volonté des autorités russes de poursuivre des activités d'espionnage économique à l'étranger. Mais la vigilance de la Sûreté de l'Etat en cette matière ne s'est pas limitée aux pays de l'Est : ce service s'est aussi montré attentif à la manière de traiter certaines demandes d'informations émanant de services « amis » concernant des transactions commerciales dans lesquelles des intérêts belges étaient en cause.

---

147 Voir en ce sens, Comité permanent R, rapport d'activités 2000, "la manière dont les services de renseignement ont traité les activités de l'ancien KGB en Belgique » (pp. 78 et suivantes,).

9.1.2. Le contre-espionnage économique.

Le 28 novembre 1997, le Comité ministériel du renseignement a chargé le collège du renseignement et de la sécurité *"d'approfondir l'analyse des menaces d'atteintes, en ce compris par l'espionnage économique, à certains secteurs socio-économiques, de formuler des propositions pour lutter contre ces menaces et d'examiner dans quelle mesure associer à ces travaux le département des Affaires économiques".*

Le collège du renseignement et de la sécurité a confié cette mission à la Sûreté de l'Etat qui a elle-même formulé les propositions d'actions suivantes dans une note du 5 février 1998 :

1) *« Faire l'inventaire des secteurs qui risquent d'être visés :*

   - *les entreprises qui ont un intérêt , économique ou technologique particulier ou qui sont vitales pour l'emploi ou les besoins de base de la population;*
   - *les instituts de recherches scientifiques, les laboratoires importants tant privés que publics, les universités et certaines écoles supérieures, les départements responsables pour les sciences et l'économie.*

2) *Déterminer et enquêter sur les menaces et leurs origines par des contacts avec les secteurs visés, et organisation d'échanges d'informations".* (Plus loin, les menaces sont ainsi décrites : "*Espionnage par des entreprises étrangères, concurrence déloyale internationale, tentative d'OPA illicite d'entreprises belges par des intervenants étrangers, etc.. Recherches d'activités clandestines de gouvernements ou administrations étrangers et leurs services de renseignement").* Selon la Sûreté de l'Etat, ne seraient donc pas inclus dans sa mission, l'espionnage industriel développé par une firme contre une autre au niveau du secteur privé national.

3) *"Elargir ou adapter les recherches dans les domaines classiques (espionnage (politique), terrorisme, extrémisme idéologique, sectes nuisibles, crime organisé, prolifération de matières NBC, protection de personnes, nombreuses tâches de recherche et d'avis administratifs,...) couverts par le service aux besoins de la protection économique et scientifique.*

4) *Sensibilisation et conseils aux institutions économiques et scientifiques quant aux mesures de sécurité à prendre(personnel, protection des données, protection physique, communications, etc.).*

5) *Assister à ou organiser des réunions de concertation avec les instances officielles concernées.*

6) *Fournir des analyses de la menace et proposer des mesures à prendre aux autorités.*

7) *Prévenir le gouvernement belge lorsque les règles du jeu propre à l'économie de marché sont délibérément faussées au détriment des intérêts belges.*

8) *Etude des législations étrangères et des aspects juridiques liés à la matière ».*

La note du 5 février 1998 se poursuit en estimant de manière minimale le besoin en personnel supplémentaire à la Sûreté de l'Etat pour réaliser cette nouvelle mission.

Le 28 octobre 1999, le ministre de la Justice a annoncé un plan de collaboration entre la Fédération des Entreprises de Belgique et les pouvoirs publics. Selon le ministre, c'était dans ce cadre que la Sûreté de l'Etat pouvait jouer un rôle proactif.

Le sujet « *protection du potentiel scientifique ou économique* » est apparu dans la liste des sujets de la Sûreté de l'Etat dés la mise en vigueur le 1er février 1999 ([148]) de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Le sujet a même été étendu à la « *protection du patrimoine industriel* » conçu comme une part du potentiel économique et qui comprend l'ensemble des activités économiques de production de biens.

En mai 2000, la Sûreté de l'Etat a rédigé un syllabus de formation sur la protection du potentiel scientifique et économique à l'intention des agents des services extérieurs chargés de cette mission. Ce syllabus est classifié « confidentiel ».

Dans son plan de sécurité de juin 2000, le gouvernement fédéral déclarait que les ministres de la Justice et de l'Intérieur poursuivraient la concertation mise en place au sein de la PCPE et qu'un groupe de travail mixte chargé de la criminalité économique prêterait attention aux modes criminels suivants : criminalité informatique, blanchiment d'argent, corruption et espionnage économique.

Entre-temps, les propositions issues de la plate-forme de concertation permanente sur la sécurité industrielle de la FEB ont été examinées en juillet 2000 par la Sûreté de l'Etat laquelle a transmis son avis au ministre de la Justice le 1er août 2000. Cet avis préconisait notamment :

- la mise en place d'une action de prévention concrétisée par la présentation d'exposés de sensibilisation auprès d'entreprises appartenant à des secteurs exposés ([149]);

- la constitution et la réactualisation d'une liste prioritaire de secteurs d'activités et de technologies de pointe permettant une protection efficace et rapide des entreprises concernées;

- le recueil de renseignements plus spécifiquement relatifs aux activités, au sein du monde économique, d'organisations sectaires, de la criminalité organisée ou d'espionnage par des puissances étrangères. Cette collecte d'information permettrait d'analyser la menace latente et la mise en place éventuelle de mesures protectrices.

Par manque de personnel et de moyens, les contacts entrepris dans les années nonante avec des responsables d'entreprises sont toutefois restés sporadiques et aucune des initiatives prises n'a vraiment été menée à son terme.

9.1.3. Les rapports et échanges d'informations sur les activités menées avant l'année 2001.

Ainsi que le souligne le Comité permanent R dans son rapport d'activités de l'année 2000 ([150]), une série de documents préalables à l'adoption de la loi organique du 30 novembre 1998 témoignent de la volonté de l'Administrateur général de la Sûreté de l'Etat de préparer son service à l'exercice de la nouvelle mission de protection du patrimoine scientifique et économique.

148 Arrêté royal du 22 janvier 1999, paru au Moniteur Belge le 30 janvier 1999.
149 Ces « *secteurs exposés* » ne sont pas autrement précisés.
150 Chapitre 7, p. 143

Les notes et propositions que la Sûreté de l'Etat a adressées le 1er août 2000 et le 31 mai 2001 aux autorités politiques témoignent également de la volonté de ce service de remplir correctement la nouvelle mission qui lui a été confiée par la loi.

Le Comité permanent R a cependant éprouvé bien des difficultés à se procurer des rapports et des documents écrits relatifs aux missions menées avant l'année 2000. Questionné à ce sujet, l'administrateur général de la Sûreté de l'Etat a notamment confirmé qu'à la fin des années 80, tous les dossiers et fiches de contre-espionnage d'une section locale avaient été détruits. Il s'agit d'un fonds d'informations concernant 10 à 15 opérations. Le Comité permanent R ne peut ici que constater et déplorer cette très malheureuse initiative.

En attendant de recevoir les directives nécessaires du Comité ministériel du renseignement et de la sécurité, la Sûreté de l'Etat n'a utilisé ses rapports qu'à des fins purement internes. De même, les discussions d'ordre général qui ont eu lieu sur le sujet avec le SGR n'ont donné lieu à aucun échange d'informations. Quelques contacts préparatoires ont été établis avec des services de renseignement étrangers, mais aucune collaboration officielle.

9.1.4. La difficulté politique de définir le potentiel scientifique et économique à protéger.

Le 31 mai 2001, la Sûreté de l'Etat a adressé au Comité ministériel du renseignement et de la sécurité une note contenant une série de propositions relatives à la définition du potentiel scientifique et économique, à l'établissement de priorités, à la détermination des menaces qui visent ce potentiel, ainsi qu'une description des missions qui devaient incomber à la Sûreté de l'Etat en cette matière. Il y était prévu que six mois après l'approbation de la note par le Comité ministériel, la Sûreté de l'Etat ferait une évaluation précises des menaces existantes et qu'elle soumettrait un plan d'action au Collège du renseignement et de la sécurité. La Sûreté devrait ensuite rendre compte de façon régulière au Collège, lequel pourrait proposer au Comité ministériel de changer ou d'adapter les priorités. Le Comité ministériel pourrait, le cas échéant, coordonner les actions dans l'éventualité d'un problème complexe qui interpelle les compétences de plusieurs services.

La Sûreté de l'Etat a proposé que le potentiel économique du pays soit défini comme suit : *« l'infrastructure et le savoir-faire à protéger et à défendre susceptibles de promouvoir une augmentation relative et soutenue de la production du travail et du capital. »* En ce qui concerne le potentiel scientifique, la Sûreté de l'Etat propose la définition suivante : « *l'infrastructure, la technologie et le savoir-faire à protéger et à défendre en matière de recherche et de développement qui sont les garants et le moteur de l'accroissement du stock de 'know-how' et qui génèrent des prestations réellement innovatrices. »*

Cette note du 31 mai 2001 énumère aussi une série d'actions que la Sûreté de l'Etat se propose d'entreprendre en la matière. Outre la recherche, l'analyse et le traitement du renseignement relatif à toute activité qui menace ou qui pourrait menacer les éléments du potentiel économique et scientifique, la Sûreté de l'Etat se propose de collaborer et d'échanger des informations en la matière avec les autorités judiciaires, les administrations fédérales, les entreprises privées et les particuliers, conformément aux articles 14, 16 et 19 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

A cet égard, la direction de la Sûreté de l'Etat se déclare disposée à mener des actions de sensibilisation à l'égard des victimes potentielles en participant, par exemple, à des forums de concertation et d'information avec les autorités chargées de leur protection. La Sûreté pourrait ainsi présenter des analyses globales et des évaluations de la menace ou procéder à la prévention et au traitement de cas ponctuels.

La Sûreté de l'Etat a présenté deux propositions de définition, l'une du potentiel économique du pays, l'autre du potentiel scientifique.

Préférant la définition de secteurs et de domaines prioritaires à l'énumération nominative de structures et d'organisations économiques et scientifiques, la Sûreté de l'Etat a proposé de considérer comme prioritaires les domaines d'activité suivants :

- les entreprises publiques autonomes (loi du 21 mars 1991),

- les organismes d'intérêt public (loi du 21 mars 1991),

- les entreprises vitales pour les besoins de la population (eau, gaz, électricité, carburant, transport, etc.),

- les entreprises, centres de recherche, universités, hautes écoles, services publics et les autres structures créées sur le plan supranational, international, fédéral et régional dont les activités ont trait à des secteurs technologiques de pointe, notamment la technologie spatiale, l'aéronautique, la santé, l'énergie, l'informatique, les télécommunications, l'environnement, la biotechnologie, la chimie et le secteur nucléaire.

Le 21 octobre 2002, l'administrateur général de la Sûreté de l'Etat a informé le Comité permanent R que le Comité ministériel du renseignement et de la Sécurité n'avait pas approuvé les propositions faites par la Sûreté de l'Etat mais qu'il avait, au contraire, créé un groupe de travail sur ce sujet. Ce groupe de travail, composé de représentants des membres du Comité ministériel et des membres concernés du Collège du Renseignement et de la Sécurité devait se réunir sur l'initiative du ministre de la Justice. Ce groupe de travail a reçu comme mission :

- d'élaborer une définition plus restrictive du potentiel scientifique et économique à protéger ;
- d'établir une liste de priorités ;
- d'y joindre une estimation budgétaire.

Au 31 décembre 2003, ce groupe de travail ne s'était pas encore réuni.

Dans une interview parue dans le journal « l'Echo » le 5 juin 2003, M. Dassen l'administrateur général de la Sûreté de l'Etat déclare que son service ne bénéficie pas encore d'une définition claire de la notion de patrimoine économique et scientifique et il pose notamment la question suivante : « *Devons-nous défendre une entreprise étrangère dont le siège est en Belgique ? Ou les intérêts et investissements de sociétés belges à l'étranger ? Il y a là un manque de clarté qui doit être comblé par le politique.* »

Par ailleurs, l'administrateur général situe les trois missions de la Sûreté de l'Etat en cette matière de la manière suivante :

- une mission d'avertissement des autorités d'un éventuel danger lié aux intérêts économiques et scientifiques ; et M. Dassen de souligner à cet égard que la privatisation d'infrastructures comme les égouts ou l'électricité, qui sont susceptibles de passer aux mains d'étrangers, n'est pas sans risque ;
- Une mission de prévention et de stimulation de la vigilance à l'égard des autorités régionales et des universités de manière à ce que les attitudes de préservation de la confidentialité de la Recherche et Développement deviennent une habitude ;
- Une mission d'enquête à l'égard des actes criminels qui ont été commis en la matière.

L'administrateur général envisage enfin que dans quelques années, la défense des intérêts économiques des Etats pourrait être gérée au niveau européen et non plus national.

Par ailleurs, la Sûreté de l'Etat maintient son avis que l'espionnage de concurrence entre deux entreprises belges ne fait pas partie de ses compétences ([151]) mais elle reconnaît que la frontière entre entreprises belges et non belges est souvent difficile à déterminer vu que beaucoup d'entreprises ont à présent un caractère multinational. L'intérêt pour une affaire devra donc être examiné au cas par cas.

9.1.5. Le protocole d'accord entre le Ministère de la Justice et la Fédération des Entreprises de Belgique (FEB) concernant la Plate-forme de concertation permanente en matière de protection des entreprises.

Le 4 décembre 2001, le ministre de la Justice a officialisé la collaboration entamée avec la PCPE au moyen d'un protocole d'accord. Un Comité permanent d'experts fédéral a été ainsi créé et composé de représentants de l'autorité (Service de la politique criminelle, Police fédérale et Sûreté de l'Etat) et d'entreprises. Ce groupe de pilotage doit servir de cadre à une concertation régulière sur les menaces dirigées contre les entreprises. Il est prévu que le ministre de la Justice, assisté par ses conseillers, par des magistrats et par les chefs des administrations concernées participe à cette concertation avec le président et l'administrateur délégué de la FEB. Le Service de la politique criminelle est chargé de l'organisation pratique de ces activités et il doit fonctionner comme bureau de contact. Les entreprises belges doivent être régulièrement invitées à des séances plénières d'information.

Des groupes de travail mixtes associant également représentants publics et privés doivent aussi accompagner et évaluer cette concertation fédérale. En fonction des priorités fixées, ils ont pour tâche de prendre des initiatives en matière de protection du potentiel scientifique et économique (tel que défini par le Comité ministériel du renseignement), d'extrémisme (tel que défini par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité), de criminalité organisée (infiltration d'organisations criminelles dans les entreprises), de délits violents, d'organisations sectaires nuisibles, de criminalité en col blanc (criminalité informatique, blanchiment d'argent, etc.) et de terrorisme. Ces groupes de travail ont aussi comme objectifs de dresser l'inventaire des besoins réciproques, de planifier et d'exécuter un plan d'action en vue de contribuer à la réalisation des initiatives précitées.
Un groupe de travail mixte privé-public « *protection du potentiel scientifique et économique du pays* » s'est mis en place le 22 mai 2002. Il est composé de délégués de la FEB et de membres de la Sûreté de l'Etat.

[151] Voir Comité permanent R - rapport d'activités 2000 – chapitre 7, p. 117

9.1.6. L'échange et la diffusion de l'information

- **vers le secteur privé.**

Le protocole d'accord entre le ministère de la Justice et la FEB a prévu qu'un canal d'information entre les autorités et les acteurs privés devrait être mis en place pour permettre l'échange rapide entre eux d'informations urgentes en cas de menaces. Ce protocole prévoit que l'échange d'informations classifiées doit se dérouler conformément à la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité

- **vers les autorités et services administratifs.**

Le 16 février 2000, le Comité ministériel du renseignement et de la sécurité a approuvé une directive en matière de communication de renseignements et de coopération entre les services de renseignement et de sécurité et les autorités et services administratifs. Cette directive recommande tant aux services de renseignement et de sécurité qu'aux services administratifs de se transmettre mutuellement dans les meilleurs délais, d'initiative ou sur demande, tous documents et renseignements nécessaires à l'accomplissement de leurs missions légales respectives, dans le respect du principe de finalité. Si, dans un contexte particulier, une coopération étroite entre les services de renseignement et de sécurité et des autorités et/ou services administratifs s'impose, les structures de coordination nécessaires seront établies en fonction des moyens disponibles et des protocoles en préciseront les modalités. La section compétente a donc entrepris de nouer des contacts avec certaines administrations fédérales et régionale comme par exemple avec le Service des affaires scientifiques, techniques et culturelles du Premier ministre (SSTC). Il n'existe cependant pas encore de structure formelle de concertation entre la Sûreté de l'Etat et ces organismes.

Dans un courrier du 5 mars 2003, l'Administrateur général déclarait à ce propos : *« Mijn inziens kan de Veiligheid van de Staat daartoe momenteel nog niet voldoende slagkracht ontwikkelen omwille van het ontbreken van voldoende mankracht en specifieke opsporingstechnieken.»* (Traduction libre : "*selon moi, la Sûreté de l'Etat ne peut encore consacrer d'efforts suffisants à cette matière étant donné le manque de moyens humains et de techniques d'enquêtes spécifiques".*)

- **vers les autorités judiciaires.**

Le 16 février 2000, le Comité ministériel du renseignement et de la sécurité a également approuvé une directive en matière de communication de renseignements et de coopération entre les services de renseignement et de sécurité et les autorités judiciaires.

9.1.7. Actions entreprises.

Bien avant la décision prise au sein de la plate-forme de concertation de la FEB en mai 2002, la Sûreté de l'Etat avait déjà entamé une série de contacts avec des responsables d'entreprises privées et publiques, de fédérations patronales, d'universités, de ministères et autres administrations publiques fédérales, régionales et communautaires. Un rapport interne daté du 20 septembre 2001 dresse le bilan des contacts établis et des analyses effectuées à cette date.

Pour chaque ministère, service ou institution contactée, le rapport mentionne la fonction du responsable avec qui l'agent de la Sûreté de l'Etat a été en relation ainsi que les compétences, matières, documents, programmes et activités susceptibles d'attirer l'attention de services de renseignement étrangers, officiels ou privés. Le rapport décrit également les préoccupations, les attentes et les besoins en matière de sécurité exprimés par les responsables des organismes contactés.

Ce rapport conclut que la mission principale de la Sûreté de l'Etat en matière de protection du potentiel scientifique et économique doit être essentiellement d'ordre préventif : il s'agit de connaître les détenteurs de « connaissances vulnérables » *(« kwetsbare kennis »)* et de les sensibiliser à l'égard des menaces d'appropriation qui peuvent se produire à leur encontre.

« Vanuit een sensibiliserende waakzame instelling dient de Veiligheid van de Staat zich te positioneren. Ze dient dus te evolueren en zich in te bedden in de bestaande structuren die in de netwerkeconomie werden opgezet om het innoverend karakter van de economische en wetenschappelijke activiteiten (kwetsbare kennis) te ondersteunen en te kanaliseren. Aldus kan ze met de vinger aan de pols op de hoogte blijven omtrent de evoluerende notie economisch en wetenschappelijk potentieel. Daarenboven is ze dan strategisch geplaatst als aanspreekpunt om eventuele behoeften te vernemen en problemen de remediëren ».

Traduction libre : *"la Sûreté de l'Etat doit se positionner comme une institution vigilante de sensibilisation. Elle doit donc évoluer et s'insérer dans les structures existantes qui ont été mises en place dans le tissu économique en vue de soutenir et de canaliser le caractère innovant des activités scientifiques et économiques (les connaissances vulnérables). C'est ainsi qu'elle peut rester en phase avec la notion évolutive de potentiel économique et scientifique. De plus, elle occupe une place stratégique pour se tenir informée des besoins éventuels et remédier aux problèmes* ».

Au mois de février 2004, des représentants de la FEB ont annoncé la création prochaine d'un nouvel organe de communication en matière de lutte contre le terrorisme. Ce système devrait permettre une meilleure collaboration entre la Police fédérale, la Sûreté de l'Etat d'une part, les entreprises d'autre part. Il s'agirait d'un point de contact grâce auquel les entreprises et les services de sécurité pourraient se prévenir mutuellement des risques d'attentats. Il n'est pas exclu d'élargir plus tard ce système à d'autres risques comme l'espionnage et la criminalité organisée. ([152])

9.1.8. Les rapports

Dans une interview parue dans le journal « l'Echo » le 5 juin 2003, l'administrateur général de la Sûreté de l'Etat déclarait que son service traitait à ce moment quelques dizaines de dossiers relatifs au patrimoine économique et scientifique.

Au cours de l'année 2001, 177 rapports d'informations ont été établis concernant la protection du potentiel scientifique et économique du pays. En 2002, ce nombre de rapports est passé à 213.

[152] De Tijd, 9/2/2004 – Le Soir, 10/2/2004.

Il s'agit de rapports relatifs à des activités de hacking, à la dissémination de virus informatiques et d'informations sensibles sur le réseau Internet. On trouve aussi des rapports concernant l'infiltration de groupes mafieux dans certains secteurs, l'activité de certaines firmes privées de renseignement économique et de lobbying, de firmes de gardiennage, de centres de recherches et d'universités, des prises de participation étrangères dans certaines entreprises belges de haute technologie, le déroulement de salons et de conférences technologiques ou scientifiques, des programmes d'échanges de chercheurs, le séjour d'étudiants étrangers dans certains centres de recherches, le commerce du diamant, etc.

9.1.9. Quelques enquêtes menées par la Sûreté de l'Etat.

Quelques enquêtes ponctuelles menées par le Comité permanent R au cours des années 2001, 2002 et 2003 ont fait apparaître que la Sûreté de l'Etat avait procédé à des constatations ou à des enquêtes en rapport direct ou indirect avec la protection du potentiel scientifique ou économique d'entreprises belges. La Sûreté de l'Etat considère notamment les activités commerciales de recueil, de traitement et d'analyse d'informations comme susceptibles de porter atteinte à ce potentiel scientifique et économique. Plusieurs enquêtes menées par ce service contiennent des indices d'activités d'espionnage économique menées par des puissances étrangères ou par des firmes privées étrangères.

- **L'enquête sur la faillite de l'entreprise Lernaut & Hauspie ([153]).**

Entre novembre 2000 et mai 2001, la Sûreté de l'Etat a rédigé 15 rapports internes sur cette affaire. Dans ce dossier, le ministère des Affaires économiques a sollicité des renseignements à la Sûreté de l'Etat avant de prendre une décision. Aucun rapport d'analyse n'a cependant été transmis aux autorités. Ce dossier contient pourtant des indices indiquant que des services de renseignement étrangers auraient pu s'intéresser, à différents moments et pour des raisons diverses, aux activités de la firme L&H.

- **Un centre de recherche belge**.

La Sûreté de l'Etat s'est intéressée à un centre de recherche à l'occasion d'un vol de matériel informatique, ainsi que de tentatives d'intrusion dans son système informatique. Plusieurs rapports portent sur les mesures de sécurité informatique mises en oeuvre par ce centre de recherche ainsi que sur les méthodes d'attaques qui ont été utilisées contre son système informatique. L'inspecteur de la Sûreté de l'Etat en charge de l'enquête a notamment suggéré que son service puisse sensibiliser le monde scientifique à la valeur de l'information piratée et aux règles de sécurité pour l'échange de données. Néanmoins, la Sûreté de l'Etat n'a pas pu pourvoir à cette tâche faute de moyens humains et de compétences techniques nécessaires. Ses rapports sont restés strictement internes au service. Aucun d'eux n'a été transmis pour information à quelque autorité politique, administrative ou judiciaire que ce soit. Le Comité permanent R a pourtant estimé que certaines informations et recommandations contenues dans les rapports de la Sûreté de l'Etat auraient pu être déclassifiées et utilement communiquées à certaines autorités ([154]).

---

153 Comité permanent R, rapport d'activités 2001, pp. 42 et suiv.
154 Comité permanent R, rapport d'activités 2001, pp. 68 et suiv.

– **Tractebel**

En juin 2000, la Sûreté de l'Etat s'est intéressée à un ressortissant russe signalé comme étant en possession d'une fausse carte d'identité belge. Cette personne était déjà connue par la Sûreté de l'Etat comme étant impliquée dans l'épineux dossier de Tractebel au Kazakhstan. Dans les conclusions de son rapport d'activités 2001 ([155]), le Comité permanent R a conclu que la communication d'informations relevantes dans cette affaire n'avait pas eu lieu, ni à destination de l'entreprise concernée, ni à destination du Premier ministre de l'époque. En avril 2001 cependant, alors que l'Inspection Spéciale des Impôts réclamait à la société TRACTEBEL plus de 150 millions d'euros pour avoir monté un ensemble de faux contrats et de fausses conventions destinés à justifier le paiements de commissions secrètes au Kazakhstan, la Sûreté de l'Etat a informé le ministre de la Justice, le magistrat national et la Police générale du Royaume du souci du secteur bancaire face au risque de pénétration ou d'infiltration des pouvoirs décisionnels de banques par des individus à la solde de groupes mafieux.

– **La firme X**

En juin 2002, la Sûreté de l'Etat a été mise au courant d'un vol d'ordinateurs, perpétré à l'encontre d'une firme spécialisée dans la fourniture de services et produits de haute technologie. Cette spin-off, créée dans le sillage d'un centre de recherche scientifique universitaire, exploite commercialement les applications scientifiques qui y ont été mises au point. La Sûreté de l'Etat a, fort opportunément, réagi à ces informations en entamant des investigations à propos des vulnérabilités apparues dans ces firmes et centres de recherches, notamment en prospectant et en sensibilisant les autorités locales et les chefs d'entreprises concernés. La Sûreté de l'Etat n'exclut pas des actes d'espionnage bien que l'hypothèse privilégiée par la police locale soit celle de vols destinés à obtenir du matériel informatique, sans égard pour le contenu des disques durs.

La Sûreté de l'Etat cherche donc à cerner le profil des auteurs des vols informatiques ainsi que leur motivation. La récente mobilisation plus accrue de la Police Fédérale en vue d'assurer la sécurité des parcs scientifiques est, semble-t-il, en partie due à l'intérêt porté par la Sûreté de l'Etat à la protection du potentiel économique et scientifique dans la région.

– **La sécurité des télécommunications d'entreprises**.

La Sûreté de l'Etat n'a jamais été consultée par qui que ce soit dans cette matière mais elle s'est déjà posé d'initiative la question des éventuels problèmes de sécurité que faisaient naître les firmes étrangères qui exécutent en Belgique des travaux dans le domaine des télécommunications. La Sûreté de l'Etat conseille d'être vigilant dans ce secteur essentiel et elle préconise certaines mesures de sécurité, comme par exemple la réalisation d'enquêtes de sécurité et l'octroi d'habilitations de sécurité.

[155] Comité permanent R, rapport d'activités 2001, pp.5 -6

C'est ainsi qu'en juin 2002, la Sûreté de l'Etat a manifesté un commencement d'intérêt aux conséquences possibles de la faillite d'une importante entreprise de télécommunication sur le potentiel économique du pays. Toutefois, la Sûreté de l'Etat ne disposant pas encore des moyens nécessaires à évaluer les dommages possibles aux infrastructures vitales du pays, elle dut donc limiter son intervention à une note d'avertissement adressée aux ministres concernés. La réponse du ministre des Télécommunications n'a pas encouragé le service à poursuivre son intervention dans cette affaire. En effet, le ministre a en effet estimé que s'agissant ici d'une affaire s'inscrivant dans le cadre d'un marché libéralisé, ce marché trouverait une solution pour un réseau aussi substantiel que celui de l'entreprise en question.

Sans vouloir contester la position du ministre des Télécommunications, le Comité permanent R a cependant estimé qu'il revenait à la Sûreté de l'Etat de veiller à ce que le potentiel économique et scientifique du pays ne soit pas menacé, même dans le cadre d'un marché libéralisé sur lequel l'autorité a peu d'emprise. Le risque existe en effet que les réseaux de télécommunication d'une entreprise en faillite, ou livrée aux vicissitudes du marché privé, puissent être pris en main par des structures maffieuses et menacer ainsi la sécurité des systèmes d'information du pays. Dans une telle matière, le Comité permanent R a donc recommandé que les ministères des télécommunications et de la Justice puissent collaborer efficacement en échangeant en permanence des informations.

- **L'incidence éventuelle de certaines prises de positions de politique étrangère de la Belgique sur la situation économique et sociale d'une entreprise étrangère établie en Belgique.**

En octobre 2003, le Comité permanent R a examiné de quelle manière la Sûreté de l'Etat avait traité des informations faisant état de répercussions possibles de positions de politique étrangère de la Belgique sur la situation économique et sociale d'une entreprise étrangère établie en Belgique. Il en ressort que des informations crédibles effectivement recueillies en ce sens ont bien été communiquées verbalement à une autorité politique mais sans que ces informations n'aient été analysées, ni vérifiées, ni confirmées par la suite.

- **L'étude de certains marchés étrangers.**

Dans son édition du 4 novembre 2003, le journal « DE TIJD » a révélé que la Sûreté de l'Etat avait entrepris l'étude du marché d'un pays émergeant étranger, de ses potentialité et de ses pièges pour les entreprises belges qui souhaitent le pénétrer. Il s'agit en effet d'un débouché déjà important pour certaines entreprises belges.

9.1.10. La consultation de la Sûreté de l'Etat à propos de l'implantation d'entreprises étrangères sur le territoire national.

Suite à une question posée en 2002 par le sénateur Marc Hordies, le Comité permanent R a adressé les questions suivantes aux services de renseignement :

- « Arrive-t-il qu'une autorité gouvernementale, qu'elle soit fédérale ou régionale, consulte votre service à propos de l'implantation d'une entreprise étrangère sur le territoire national ?
- A l'inverse, vous arrive-t-il de communiquer spontanément des renseignements à une autorité gouvernementale, qu'elle soit fédérale ou régionale, à propos de l'implantation d'une entreprise étrangère sur notre territoire ?

– Dans l'affirmative, dans quelles circonstances ces renseignements vous sont-ils demandés et/ou transmis ? D'office ou occasionnellement ? De quels types de renseignements s'agit-il ? S'agit-il de renseignements relatifs à la couverture éventuelle d'activités mafieuses, de blanchiment d'argent ou de corruption, etc. ?

Le même courrier demandait aux services de renseignement de citer des exemples banalisés de renseignements de ce genre qui auraient été demandés ou communiqués à une autorité gouvernementale.

L'administrateur général adjoint de la Sûreté de l'Etat a fait savoir que son service n'était pas consulté par les autorités régionales ou fédérales à propos de l'implantation d'entreprises étrangères en Belgique. Il a attiré l'attention du Comité sur le fait que de grandes entreprises d'Europe de l'Est s'installaient souvent en Belgique avec l'aide de bureaux d'avocats spécialisés. Ces entreprises y fixent souvent leur siège administratif.
Une enquête que le Comité permanent R a réalisée en 2001 avait par ailleurs fait apparaître que l'éventualité d'une intervention de la Région wallonne dans le financement d'une entreprise étrangère en difficulté n'avait suscité aucune réaction de la part de la Sûreté de l'Etat alors que ce service était en possession d'indices permettant de suspecter que cette entreprise couvrait des activités de renseignement, d'espionnage, voire de terrorisme ([156]).

La Sûreté de l'Etat se déclare surtout attentive à la délivrance des cartes de travail des administrateurs des grandes entreprises est-européennes actives dans les secteurs du pétrole et des matières premières. Dans ce contexte, ce service collabore avec divers ministères fédéraux et services régionaux.

9.1.11. L'attitude de la Sûreté de l'Etat à l'égard des services de renseignement privés.

La Sûreté de l'État est quelquefois appelée à délivrer des avis préalables à l'agréation de détectives privés et de responsables de firmes de gardiennage. Ce service estime qu'il lui est très difficile de donner une définition correcte du secteur du renseignement privé puisque le traitement d'informations est une part essentielle de l'activité de nombreux secteurs de l'économie.

L'attention de la Sûreté de l'État a pourtant été attirée par quelques firmes privées de renseignement actives en Belgique. Il s'agit d'enquêtes menées sur des affaires d'espionnage économique ou industriel, sur des activités de lobbying, sur certaines sectes. Certaines firmes sont soupçonnées d'agir pour le compte de services de renseignement de pays étrangers.

En mai 2001, la Sûreté de l'Etat a proposé au Comité ministériel du renseignement et de la sécurité une définition de l'espionnage économique et de l'espionnage de concurrence. Seul l'espionnage économique, relevant d'Etats étrangers, relèverait de la compétence de la Sûreté de l'Etat.

Mais ce service a aussi proposé d'être investi de la mission d'envisager parmi les menaces dirigées contre le potentiel scientifique et économique, certaines activités commerciales de recueil, de traitement et d'analyse d'informations d'une part, la fabrication et la diffusion d'informations en vue de désorganiser certains secteurs essentiels de l'économie d'autre part.

---

[156] Rapport d'activités 2001 : rapport de l'enquête sur la manière dont la Sûreté de l'Etat a assuré le suivi de l'abattoir islamique de Gembloux, pp. 139 et suiv.

9.1.12. Les moyens humains affectés à la protection du potentiel scientifique et économique.

La nouvelle section créée parmi les services extérieurs de la Sûreté de l'Etat spécifiquement chargée de la protection du potentiel économique et scientifique a été contrainte de suspendre ses activités entre le mois d'octobre 2001 et le mois de février 2002 suite à des réaffectations temporaires d'agents, provoquées par le surplus de missions occasionné par la protection des personnalités présentes en Belgique lors du sommet européen de Laeken et par les attentats du 11 septembre 2001 aux Etats-Unis. Ces affectations temporaires ont été levées par la note de service du 8 février 2002 et la section spécialement chargée de la protection du potentiel scientifique et économique a alors vu ses effectifs augmentés. Au 1er mars 2003 cependant, le cadre de cette section n'était toujours pas rempli.

Les autres sections des services extérieurs de la Sûreté de l'Etat participent aussi à cette mission car elles sont habilitées à recueillir et à transmettre des informations en rapport avec le potentiel scientifique et économique lorsque les menaces émanent soit des pays, soit des milieux extrémistes, sectaires ou criminels qu'elles traitent.

Depuis septembre 2000, le service d'analyse chargé de la législation en matière d'armes, de la prolifération et des trafics d'armes, est aussi chargé de recevoir et de traiter tous les rapports relatifs à la protection du potentiel scientifique et économique.

Le nouvel administrateur général de la Sûreté de l'Etat a entrepris une réforme de ses services dans le courant de l'année 2003. Désormais l'ensemble des services extérieurs et des services d'analyse devraient être réorganisés en directions géographiques composées chacune d'analystes et d'agents des services extérieurs. Chaque direction aurait la mission de recueillir et d'analyser le renseignement sur l'ensemble des menaces qui émanent d'une région déterminée du monde et qui sont de la compétence générale de la Sûreté de l'Etat (l'espionnage, l'extrémisme idéologique, le terrorisme, la criminalité organisée, les sectes et la prolifération d'armes). L'espionnage scientifique et économique devrait donc à présent être traité par chaque direction géographique selon l'origine géographique des activités d'espionnage détectées (qui peuvent notamment avoir des « *conséquences déstabilisatrices sur le plan politique ou socio-économique* »). Des experts des services d'analyse et des services extérieurs devraient par ailleurs assurer la coordination des renseignements recueillis sur certains thèmes spécifiques comme par exemple la protection du potentiel scientifique et économique.

Dans une interview parue dans le journal « l'Echo » le 5 juin 2003, l'administrateur général de la Sûreté de l'Etat déclare qu'environ un tiers à la moitié des 70 nouveaux agents qui devraient être engagés dans un avenir proche seront affectés à cette matière. Ils auront des profils de financiers, d'économistes, d'informaticiens et d'analystes géopolitiques à orientation économique.

9.2. Que fait le SGRS en cette matière?

Le SGRS n'a officiellement aucune compétence légale pour s'occuper de la protection du potentiel scientifique et économique du pays. Ce service est néanmoins investi de certaines missions qui peuvent être mises en rapport avec cette matière.

9.2.1. La gestion de certains brevets classifiés.

Ainsi, dans le cadre de la loi du 10 janvier 1955 sur la propriété industrielle, une section du SGRS assure la gestion des informations et brevets “classifiés” conjointement avec le ministre des Affaires économiques pour contrôler les conditions d’exploitation, d’inventions et de mise en oeuvre des secrets de fabrique portés à la connaissance de sociétés commerciales, dans le cadre de leurs activités spécifiques au profit de la Défense nationale ou de l’OTAN. Il s’agit en l’occurrence d’appliquer les procédures inhérentes au dépôt, à la gestion et la levée du secret des brevets, des inventions et des informations “classifiés” qui, à ce titre, ne peuvent être divulgués conformément à la loi.

Cette section établit et diffuse des directives de sécurité industrielle et contrôle leur application auprès des sociétés industrielles installées sur le territoire national. Si l’installation est située dans un autre pays, le SGRS veille à ce que ce contrôle se fasse dans le pays concerné par l’autorité nationale compétente de ce pays. Le SGRS agit de la même manière sur le territoire national pour les brevets “classifiés” par un Etat étranger, dans le cadre de l’article 12 de la loi en question.

9.2.2. Les enquêtes de sécurité.

Le SGRS effectue également les enquêtes en vue de l’octroi des habilitations de sécurité aux firmes, à leurs administrateurs et à leur personnel dans le cadre de leurs activités spécifiques au profit de la Défense nationale ou de l’OTAN. La finalité de ces enquêtes est de vérifier l’intégrité des administrateurs et du personnel de ces firmes, aussi bien sur le plan de la fiabilité, de la loyauté et de la discrétion que sur les plans financier et commercial.

9.2.3. La consultation à propos d’entreprises étrangères s’établissant en Belgique.

Sur demande du sénateur Hordies en 2002, le Comité permanent R a aussi posé la question de la consultation éventuelle du SGRS à propos d’entreprises étrangères s’établissant en Belgique.

La réponse de ce service fut claire et précise. Le SGRS n’a jamais été consulté par autorité gouvernementale, qu’elle soit fédérale ou régionale, à propos de l’implantation d’une entreprise étrangère sur le territoire national. Dans le sens inverse, le SGRS n’a jamais fourni d’office des renseignements relatifs à une telle implantation.

9.2.4. L’attitude du SGRS à l’égard des services de renseignement privés.

D’une manière générale, *le SGRS* ne se sent pas concerné par la problématique des services de renseignement privés qu’il considère comme seulement liée à la protection de potentiel scientifique et économique, matière qui n’entre pas dans ses compétences légales.

Le SGRS déclare n’avoir jamais mené d’investigation de quelque nature que ce soit à propos de l’une ou l’autre de ces firmes de renseignement privées. Si le SGRS était au courant de ou suspectait des faits d’espionnage économique ou scientifique en Belgique imputables à des firmes de renseignement privées, il en informerait immédiatement la Sûreté de l’Etat eu égard à sa compétence spécifique en cette matière. Si toutefois des intérêts militaires étaient concernés par l’affaire, le SGRS en resterait saisi vu sa compétence en matière de contre-espionnage.

En ce qui concerne les Sociétés Militaires Privées, le Comité permanent R pense que celles-ci auront un rôle de plus en plus importants dans les conflits à venir et que les services de renseignements belges, en particulier le SGRS, devront tenir compte de ces nouveaux acteurs sur leurs futurs terrains d'opérations par exemple humanitaires, et dans le cadre de conflits armés à venir.

9.3. L'intérêt de la Défense nationale pour la veille technologique.

Au mois de mai 2002, un mémoire consacré à la veille technologique (« *de technologische voorhoede* » en Néerlandais) a été présenté par le major d'aviation Fernand Rouvroi à l'Institut royal supérieur de Défense (IRSD). Cet officier met en évidence le rôle capital que joue la technologie pour la défense et la sécurité. « *L'évolution technologique crée de nouvelles opportunités pour répondre aux menaces diverses et évolutives. Mais elle engendre également de nouvelles menaces, ce qui hisse la technologie à un niveau d'importance stratégique.* » Et l'auteur de souligner à cet égard le fossé grandissant entre l'Europe et les Etats-Unis. *« Pour relever ces défis, il convient d'utiliser tous les moyens disponibles, et en particulier la veille technologique. Apparue voici dix ans, cette discipline, qui se situe dans le concept plus général de l'intelligence économique, est un processus qui s'apparente au cycle du renseignement militaire, et s'applique aux nouvelles technologies en développement»*. Le major Rouvroi définit la veille technologique « comme le processus de collecte, de traitement et de diffusion de l'information technologique au sens large, en vue d'appuyer la prise de décision stratégique relative aux matériels présents et futurs de la défense. Il propose par conséquent de créer au sein de la Défense nationale une structure élaborée de veille technologique. Il devrait s'agir d'un *« réseau où certains acteurs seraient responsables de la surveillance d'un secteur particulier et collecteraient les informations relatives à ce secteur. Ces dernières seraient analysées par d'autres acteurs qui en feraient la synthèse. Celle-ci serait rangée de façon thématique sur le réseau de manière à garantir un accès plus facile et plus concret à l'information.* » Le major Rouvroi propose ce modèle en tenant compte de l'expérience des firmes et des organismes qui pratiquent déjà la veille technologique et à l'expertise desquels il envisage d'avoir recours.

Le Comité permanent R salue cette étude et souhaite qu'elle soit prise en considération avec l'intérêt qu'elle mérite par la Défense nationale.

10. CONCLUSIONS.

10.1. La Sûreté de l'Etat.

Près de cinq années après que la loi du 30 novembre 1998 organique des services de renseignement et de sécurité lui ait été attribuée la mission de protéger le potentiel scientifique et économique du pays, l'administrateur général de la Sûreté de l'Etat reconnaît l'important retard accusé en ce domaine par rapport aux voisins européens. Néanmoins, la Sûreté de l'Etat met progressivement en place les outils nécessaires à l'exercice de cette tâche de manière opérationnelle. Ainsi,

- Dans un premier temps, une section des services extérieurs a été dédiée de manière spécifique à cette mission ;

- Les autres sections des services extérieurs devraient bientôt être également habilitées à recueillir des informations en rapport avec le potentiel scientifique et économique selon l'origine géographique des menaces.
- Le service d'analyse compétent pour traiter la prolifération et les trafics d'armes a également été chargé de traiter l'information recueillie par les services extérieurs en matière de protection du potentiel scientifique et économique.
- Dans une nouvelle phase de restructuration, les services extérieurs et les services d'analyse ont été réorganisés en directions géographiques, chacune d'elles étant compétente pour l'ensemble des matières traitées par la Sûreté de l'Etat.
- La Sûreté de l'Etat a adressé au Comité ministériel du renseignement et de la sécurité une note contenant une série de propositions relatives à la définition du potentiel scientifique et économique, à l'établissement de priorités, à la détermination des menaces qui visent ce potentiel, ainsi qu'une description des missions qui devaient incomber à la Sûreté de l'Etat en cette matière.
- La Sûreté de l'Etat est concernée par le protocole d'accord passé entre le ministère de la Justice et la FEB qui met en place un canal d'information entre les autorités et les acteurs privés.
- Dans ce cadre, la Sûreté de l'Etat a entamé une série de contacts avec des responsables d'entreprises privées et publiques, de fédérations patronales, d'universités, de ministères et d'autres administrations publiques en vue de les sensibiliser aux menaces affectant les potentiels scientifiques et économiques dont ils ont la charge.
- Dans une seconde phase, la Sûreté de l'Etat envisage de s'adresser à des grandes entreprises stratégiques afin de s'informer sur leurs besoins et attentes en matière de protection.
- Dans ce cadre, la Sûreté de l'Etat a mené quelques enquêtes ponctuelles, notamment dans des cas où des entreprises ont été victimes de vols de données.
- La Sûreté de l'État est consciente du danger potentiel que représente le développement des firmes privées de renseignement. Elle s'intéresse quelquefois à de telles firmes lorsqu'elle délivre des avis préalables à l'agréation de détectives privés et de responsables de firmes de gardiennage. Ce service n'a toutefois pas encore développé d'analyse stratégique sur l'essor de ce nouveau secteur d'activités commerciales.
- Depuis 2003, la Sûreté de l'Etat semble adopter une attitude plus proactive en matière économique puisqu'elle a entrepris l'étude et l'analyse d'un important pays dans lequel des entreprises belges désirent exporter et se développer.

L'implication de la Sûreté de l'Etat dans la protection du potentiel scientifique et économique du pays est cependant contrariée par le fait que ce service,

- n'a pas gardé trace des rapports et contacts établis par des « anciens » avec les milieux économiques avant 1998 et n'a donc pu en tirer profit ;
- a détruit certaines archives relatives à des affaires d'espionnage provoquées par d'anciens pays du bloc de l'est avant la chute du rideau de fer ; le Comité permanent R ne peut ici que constater et déplorer cette très malheureuse initiative sur laquelle il se propose de mener une enquête distincte de la présente ;
- n'a toujours pas encore reçu les directives du Comité ministériel définissant le potentiel scientifique et économique à protéger ainsi que le prescrit l'article 7, 1° de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité; ce Comité n'a, en effet, pas approuvé les propositions faites par la Sûreté de l'Etat ; il a cependant créé un groupe de travail sur ce sujet qui, au 31 décembre 2003, ne s'est toujours pas réuni ;
- a dû consacrer la plupart de ses moyens humains au surplus de missions occasionné par la protection des personnalités présentes en Belgique lors du sommet européen de Laeken et par les attentats du 11 septembre 2001 aux Etats-Unis ;
- ne dispose pas d'officiers de liaison à l'étranger ;

- doit tenir compte que la plupart des grandes entreprises stratégiques établies en Belgique font partie de consortiums internationaux ;
- est confronté aux lois du marché et de la concurrence dans le cadre d'une société fondée sur l'accès ouvert à tous les marchés, la libre entreprise, la mondialisation et la déréglementation ;
- n'est pas consultée par les gouvernements des régions wallonne, flamande et bruxelloise en cas d'implantation d'entreprises étrangères en Belgique ni associée à leurs démarche de promotion des intérêts économiques belges à l'étranger ;
- n'obtient pas de collaboration décisive en ce domaine de la part des services correspondants étrangers étant donné que la protection du potentiel scientifique et économique du pays demeure encore une matière touchant de près aux intérêts strictement nationaux.

La nouvelle mission de défense du potentiel économique et scientifique pose incontestablement des problèmes de définition et de délimitation concrètes non seulement à la Sûreté de l'Etat, mais également aux responsables politiques.

Ces problèmes se doublent en ce qui concerne la Sûreté de l'Etat d'une difficulté à définir et à appliquer de manière rigoureuse une stratégie du renseignement principalement en ce qui concerne le traitement et l'analyse de l'information.

La communication en temps opportun de renseignements stratégiques pertinents reste un domaine où des efforts incontestables doivent porter.

10.2. Le SGRS.

Ce service ne possède aucune compétence légale pour enquêter sur les menaces à l'égard du potentiel scientifique et économique en général. Toutefois, si des intérêts militaires sont concernés, le SGRS s'en occupe vu sa compétence en matière de contre-espionnage.

Le SGRS s'occupe aussi de la gestion de brevets classifiés et d'enquêtes de sécurité dans des entreprises travaillant pour la Défense nationale. Ce service possède donc une expertise en matière de sécurité dans les entreprises qui ne doit pas être négligée. Il s'agit d'un savoir-faire qui pourrait lui permettre de collaborer avec la Sûreté de l'Etat.

Par ailleurs, certaines propositions intéressantes se font jour à la Défense nationale en matière de veille technologique. L'intérêt porté par cette institution à cette discipline nouvelle, allié au savoir-faire du SGRS, constitue une réserve de compétences qui peut être utile à la protection et au développement du potentiel scientifique et économique du pays.

11. RECOMMANDATIONS.

11.1. Au niveau législatif

- **Définir ce qu'est l'information protégée et l'espionnage économique.**

Une définition légale du secret des entreprises et de l'espionnage économique apparaît en effet comme un élément essentiel de la sécurité économique.

Le Comité permanent R est néanmoins conscient de la difficulté de définir les notions de service de renseignement privé, d'espionnage et de secrets scientifiques et économiques à protéger dans le contexte actuel de la libre entreprise et de la société de l'information dominée par les progrès technologiques. La législation américaine pourrait cependant inspirer le législateur belge pour élaborer une définition légale du secret des entreprises et de l'espionnage économique. Aux Etats-Unis, la « *proprietary information* » est de l'information non disponible dans le domaine public et pour laquelle le propriétaire a pris des mesures de protection. Il s'agit d'informations que le droit américain protège comme « *trade secrets* »

- **Mieux circonscrire le cadre légal des enquêtes préalables à l'embauche**.

Le Comité permanent R estime également qu'à l'instar des enquêtes pour l'octroi des habilitations de sécurité, les enquêtes préalables à l'embauche de salariés devraient être mieux réglementées dans le sens d'une meilleure transparence de la procédure. Ainsi un employeur ne devrait pas être autorisé à recueillir ou à faire recueillir des informations relatives à l'état civil, à la conduite, à la moralité et à la solvabilité d'un de ses salariés ou d'un postulant à l'insu de cette personne. Le commanditaire de l'enquête devrait en toute circonstance avoir l'obligation d'informer l'intéressé sur les procédures utilisées pour recueillir et traiter les données personnelles dans le cadre du recrutement. De même, les informations ainsi recueillies devraient être mises à la disposition de la personne concernée pour lui permettre de les rectifier ou de présenter ses observations.

11.2. Au niveau gouvernemental fédéral

- **Définir le potentiel scientifique et économique à protéger.**

Le Comité permanent R est toujours conscient de la difficulté de protéger les secrets scientifiques et économiques dans le contexte actuel de la société de l'information dominée par les progrès technologiques, et caractérisée autant par son internationalisme que par son ouverture d'esprit scientifique. Le Comité permanent R est tout aussi conscient de la difficulté de définir le rôle que la Sûreté de l'Etat doit jouer dans la protection du potentiel scientifique et économique du pays dans le cadre d'une société fondée sur l'accès ouvert à tous les marchés, la libre entreprise, la mondialisation et la déréglementation.

Le Comité permanent R recommande donc une fois de plus que cet obstacle soit rapidement levé pour permettre à la Sûreté de l'Etat de remplir avec plus de détermination sa nouvelle mission légale.

- **Etablir un mécanisme de contrôle et de surveillance des investissements étrangers dans les domaines considérés comme stratégiques pour la Belgique.**

Le Comité permanent R estime qu'à l'instar de l'exemple français, la Sûreté de l'Etat devrait être associée à un mécanisme de contrôle et de surveillance des investissements étrangers dans les domaines considérés comme stratégiques, comme par exemple les technologies de l'information.

- **Reconnaître l'étendue de l'essor du renseignement privé, définir cette notion et ses règles.**

A l'instar de l'exemple français, le Comité permanent R recommande l'adoption en Belgique d'une référence de normalisation pour « *toute prestation concourant à la mise en place et à l'alimentation d'un dispositif de surveillance active de l'environnement technologique, commercial, économique, sociologique, géopolitique, concurrentiel, juridique, réglementaire, normatif, etc., que cette prestation soit réalisée en interne ou en externe, qu'elle fasse l'objet d'une transaction marchande ou non, que l'entité qui la réalise soit publique, parapublique ou privée* ».

Le Comité permanent R estime que cette norme devrait en outre définir les règles déontologiques régissant de telles prestations.

- **Donner à la Sûreté de l'Etat les moyens légaux, techniques et humains appropriés.**

Le Comité permanent R rappelle aussi que la Sûreté de l'Etat ne pourra remplir convenablement les nouvelles missions qui lui ont été assignées par la loi du 30 novembre 1998, notamment la protection du potentiel scientifique et économique, si elle ne reçoit pas les moyens légaux, techniques et humains appropriés :

- les moyens légaux techniques, c'est-à-dire un cadre légal pour procéder de manière sélective et strictement contrôlée à des repérages, à des écoutes et à des interceptions de communications ;
- les moyens humains, c'est-à-dire des experts externes, des économistes, des juristes, des informaticiens, des ingénieurs en télécommunications, des spécialistes en cryptographie, des analystes, etc. ;

Il conviendrait par ailleurs d'envisager la mise en place d'un service officiel chargé de l'ensemble de la problématique de la sécurisation de l'information.

Si les besoins de sécurité du secteur privé ne sont pas suffisamment pris en compte par les autorités publiques et par les services de renseignement officiels, soit les entreprises et les laboratoires de recherche continueront à sous-estimer les risques qu'ils courent, soit ils se tourneront davantage vers ces firmes privées de renseignement et de sécurité dont les activités, l'éthique et le contrôle démocratique ne font pas encore l'objet d'un cadre juridique suffisamment défini.

- **Mieux associer la Sûreté de l'Etat au contrôle des détectives privés**.

Dans le cadre de la législation actuelle sur la profession de détective privé, le Comité permanent R recommande que la Sûreté de l'Etat soit davantage consultée par le ministre de la Justice à propos des personnes qui se proposent d'exercer ce métier.

Néanmoins, à l'instar de la procédure d'octroi des habilitations de sécurité, il conviendrait d'ouvrir une possibilité de recours sur le fond à la personne qui aurait fait l'objet d'un avis ou d'un rapport négatif. Le seul recours possible actuellement est un recours en annulation devant le conseil d'Etat.

De même, dans le cadre de la directive ministérielle MFO-4 prise par le ministre de l'Intérieur le 4 novembre 2002, le Comité permanent R recommande que la Sûreté de l'Etat soit aussi invitée à informer systématiquement ce ministre des cas où, à sa connaissance, un détective privé serait compromis dans une affaire d'espionnage économique ou concurrentiel, ou dans d'autres activités susceptibles de constituer une menace au sens des articles 7 et 8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

– **Reconnaître et conforter le rôle du SGRS en matière de sécurité des secteurs économiques liés à la Défense nationale ; encourager la collaboration entre ce service et la Sûreté de l'Etat.**

Le SGRS dispose d'une expertise acquise indéniable dans la protection de certains secteurs économiques et scientifiques en rapport avec la Défense nationale. Il y a lieu d'en tenir compte pour associer plus largement le SGRS à la protection du potentiel scientifique et économique, en collaboration avec la Sûreté de l'Etat.

– **Sensibiliser les gouvernements des Régions au rôle que les services de renseignements sont ainsi susceptibles de jouer dans la protection des intérêts scientifiques et économiques régionaux.**

11.3. Au niveau opérationnel

- **Elaborer les directives internes nécessaires à l'exécution de cette nouvelle mission**

A la connaissance du Comité permanent R , la Sûreté de l'Etat n'a encore élaboré aucune directive interne définissant les règles générales pour exécuter sa nouvelle mission de protection du potentiel scientifique et économique. Ceci semble pourtant un préalable nécessaire à une bonne exécution de la mission.

– **Ne pas négliger les PME.**

Sans nécessairement faire sien cet avis selon lequel, suite à l'internationalisation de l'économie, il n'existerait pratiquement plus de patrimoine économique proprement belge, le Comité permanent R est d'avis que la protection des Petites et Moyennes Entreprises mérite l'attention toute particulière de la Sûreté de l'Etat. Les PME sont souvent innovatrices et créatrices de technologies nouvelles, voire sensibles, ne serait-ce qu'au niveau de la sous-traitance. Ces entreprises sont par contre peu informées des risques auxquels elles peuvent être confrontées et elles ne sont par conséquent pas sensibilisées (ou trop peu) aux règles de sécurité.

Le Comité permanent R recommande par conséquent à la Sûreté de l'Etat de ne point négliger le contact avec les PME dans l'exercice de sa mission de protection du potentiel scientifique et économique.

– **Etendre la collaboration internationale**.

Le Comité est conscient de la difficulté de collaborer avec des services étrangers sur la protection du potentiel scientifique et économique qui est éminemment perçue comme liées à des intérêts purement nationaux et qui peuvent être en contradiction avec ceux d'Etats pourtant réputés amis.

Le Comité permanent R estime que l'internationalisation de l'économie, la construction européenne, de même que l'interdépendance de plus en plus grande des intérêts économiques nationaux par rapport à des groupes industriels et financiers internationaux devraient conduire les services de renseignements européens à envisager cette matière au-delà des frontières nationales. La grande criminalité économique et financière peut avoir des conséquences économiques et sociales extrêmement graves non seulement au niveau d'une région ou d'un pays mais aussi d'un ensemble de pays.

Les récents événements mondiaux démontrent par ailleurs que la criminalité économique et financière (par exemple, le blanchiment d'argent) de même que l'espionnage scientifique et économique peuvent être liés aux activités de groupes mafieux et / ou terroristes aux multiples ramifications internationales.

Par ailleurs, la Sûreté de l'Etat devrait être mise en mesure de pouvoir collecter des informations à l'étranger par ses propres moyens.

– **Améliorer la collaboration avec les autorités judiciaires.**

Enfin le Comité permanent R réitère les recommandations qu'il a formulées à l'issue de son enquête « *sur la manière dont les services de renseignement ont réagi à propos d'éventuels faits d'espionnage ou de tentative d'intrusion dans le système informatique d'un centre de recherche belge* ». A savoir que la conclusion d'un accord entre les autorités judiciaires et les services de renseignement, dans le cadre de l'article 14 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, devrait notamment viser à faciliter les échanges d'informations sur l'espionnage militaire, économique et scientifique entre ces autorités. Dans un tel cadre, le Comité permanent R suggère que le Collège des Procureurs généraux envisage la création d'une notice spécifique relative à l'espionnage économique et scientifique. Celle-ci s'ajouterait aux notices classiques du droit pénal commun.

– **Profiter des enquêtes de sécurité pour sensibiliser les détenteurs d'habilitations de sécurité aux règles de sécurité et aux réalités de l'espionnage, notamment économique.**

Le Comité permanent R recommande que chaque enquête de sécurité menée en application de la loi du 11 décembre 1998 relative à la classification et aux enquêtes de sécurité comprenne un entretien de sensibilisation et de mise en garde de la personne concernée aux règles de sécurité et aux réalités de l'espionnage, notamment économique

CHAPITRE 2: RAPPORT DE L'ENQUETE DE CONTROLE SUR LES EVENTUELLES ACTIVITES DE LA SURETE DE L'ETAT CONCERNANT LA PROTECTION DU POTENTIEL ECONOMIQUE ET SCIENTIFIQUE LORS DE LA FAILLITE DE LA FIRME KPNQWEST.

1. INTRODUCTION

Depuis le 1er janvier 1998, le marché des télécommunications en Belgique est complètement libéralisé, de sorte que n'importe quelle entreprise privée ou publique peut désormais y exploiter un réseau et fournir des services de télécommunication moyennant respect de conditions fixées par la loi et ses arrêtés d'exécution.

C'est dans ce contexte que la société *KPNQwest* fut fondée en novembre 1998 par les opérateurs de télécommunication néerlandais *KPN* et américain *Qwest.* Spécialisée dans la transmission de données par l'Internet, cette société gérait un réseau européen de fibres optiques long de 25.000 km qui reliait les grandes villes européennes de dix-huit pays entre elles et au reste du monde. Ce réseau particulièrement performant assurait une grande part (de 45 à 60 % selon les sources) du trafic des données électroniques en Europe. *KPNQwest* comptait quelque 100.000 entreprises clientes parmi lesquelles de nombreux fournisseurs d'accès régionaux à l'Internet mais aussi d'importantes entreprises comme *KLM*, *AOL, NOKIA, Tiscali, Ernst & Young, Hewlett-Packard,* la société boursière *Euronext*, le groupe américain *Dell*, *Teleglobe,* etc. Début 2002, *KPNQwest* reprit l'exploitation du réseau *EBONE* de la société américaine *Global Tele System*.

KPNQwest disposait d'une filiale belge *KPNQwest Assets Belgium NV* dont le centre de contrôle, établi à Hoeilaart, employait quelques 350 personnes. Cette société reçut du ministre des télécommunications son autorisation d'exploiter un réseau en Belgique le 21 avril 1999. Ce réseau s'étendait sur 350 km. Des entreprises belges comme *Belgacom,* … y étaient reliées.

Cependant, après quatre ans d'existence, *KPNQwest* subit de plein fouet la crise du secteur des télécommunications. Fortement endettée (on parle d'une dette de 1,8 milliards d'euros) cette société fut déclarée en faillite par un tribunal néerlandais à la fin du mois de mai 2002.

Dès que l'ampleur des difficultés financières de *KPNQwest* a permis de prévoir une faillite imminente de la firme, la question s'est posée de l'impact que pourrait avoir l'arrêt de ses réseaux en Europe sur les entreprises clientes. L'analyse des articles de presse de l'époque montre que les clients les plus importants de *KPNQwest* avaient déjà élaboré des plans pour se connecter à d'autres transmetteurs de données. Mais on prévoyait que la résorption du réseau allait néanmoins provoquer des perturbations, des saturations et des ralentissements du trafic.

Après avoir vainement recherché des repreneurs possibles, les curateurs de *KPNQwest* ont décidé de fermer le réseau belge le 19 juillet 2002. Plus que les grands groupes, dont la plupart disposaient déjà de systèmes alternatifs, ce sont les petits utilisateurs commerciaux qui semblent avoir été le plus pénalisés dans leurs connexions à la toile et à leur courrier électronique.

A partir de ce moment, le réseau européen de *KPNQwest* fut morcelé en différents réseaux nationaux ou transnationaux repris chacun par différents groupes financiers ou de télécommunication. Ainsi par exemple, le réseau de Russie et d'Europe Centrale fut repris par le holding russe *Menatep* au mois d'août 2002. Les réseaux français et italiens furent repris par le groupe suédois *Telia.*

En novembre 2002, l'opérateur néerlandais *KPN* a racheté et repris l'exploitation de l'ancien réseau de *KPNQWest* en Belgique, aux Pays-Bas, en Allemagne, en Grande Bretagne ainsi que la connexion avec les Etats-Unis.

Le Comité permanent R a estimé que la faillite de *KPNQwest* et l'arrêt de son réseau de fibres optiques pouvaient porter préjudice au potentiel scientifique et économique de notre pays et qu'à ce titre, cette affaire était susceptible d'intéresser la Sûreté de l'Etat.

2. PROCÉDURE

Le 14 juin 2002, la Commission de suivi du Sénat a approuvé une demande d'enquête introduite par le sénateur Marc Hordies « *sur la manière dont la Sûreté de l'Etat protège notre patrimoine économique ainsi que nos réseaux de communication (cfr ECHELON) dans le cas de faillite et du rachat éventuel de KPNQwest* ».

Faisant suite à cette demande, le Comité permanent R a décidé le 28 juin 2002 d'ouvrir une enquête de contrôle sur les éventuelles activités de la Sûreté de l'Etat concernant la protection du potentiel économique et scientifique lors de la faillite de la firme KPNQwest.

Le président du Sénat en a été averti le 4 juillet 2002.

Une apostille a été adressée au chef du Service d'enquêtes le 30 juillet 2002.

Le ministre de la Justice a été averti de l'ouverture de l'enquête le 12 août 2002.

Les devoirs de l'enquête ont été exécutés au cours du mois de septembre 2002.

Le Service d'enquêtes R a transmis son rapport au Comité permanent R le 15 octobre 2002.

Le présent rapport a été approuvé le 12 décembre 2002.

3. CONSTATATIONS DU COMITÉ PERMANENT R

Le Comité permanent R a demandé à son Service d'enquêtes de procéder à toutes les auditions et investigations nécessaires afin de savoir si la Sûreté de l'Etat s'intéressait (ou s'était intéressée) à la firme KPNQwest et aux causes de sa faillite. Les constatations du Comité permanent R résultent aussi e la prise de connaissance d'articles de presse, de documents parlementaires, des réponses orales et écrites de la Sûreté de l'Etat ainsi que des documents qui lui ont été fournis par ce service.

Le 30 août 2002, la Sûreté de l'Etat a fait parvenir au Service d'enquêtes R une note décrivant par ordre chronologique son intervention dans le cadre de la faillite de *KPNQwest.* Parmi les documents que la Sûreté de l'Etat a joints à sa réponse, figurent les copies des documents suivants :

- une apostille du service d'études E2 datée du 7 juin 2002,

- une note du 10 juin 2002 adressée aux ministres de la Justice, des Télécommunications, des Affaires économiques, de la Mobilité et du Transport,

- deux rapports du service extérieur A 12, datés du 12 juin 2002.

- une copie de la réponse adressée le 19 juin 2002 à la Sûreté de l'Etat par le ministre des Télécommunications.

Ces documents ne sont pas classifiés.

3.1. Chronologie de l'enquête de la Sûreté de l'Etat

Dès que la presse commença à publier des articles concernant la menace de faillite de *KPNQwest*, le service d'études compétent pour la protection du potentiel scientifique et économique reconnut immédiatement l'intérêt intrinsèque de cette affaire et décida de la suivre pas à pas. Cet intérêt de la Sûreté de l'Etat était justifié par sa mission de protection du potentiel scientifique et économique du pays. Ainsi commença le recueil d'informations aussi bien dans les sources ouvertes (presse nationale et internationale) que via la section opérationnelle chargée de cette matière dans les services extérieurs.

Les démarches suivantes furent immédiatement entreprises en concertation entre le service d'études et le service opérationnel :

- Une apostille fut rédigée le 7 juin 2002 par le service d'études pour commencer une enquête sur la menace de faillite de *KPNQwest* et sur les risques y étant liés.

- Le service extérieur prit contact avec un responsable de *KPNQwest.* L'intention de la Sûreté de l'Etat était de pouvoir mieux évaluer la situation ainsi que les dommages possibles que la fermeture éventuelle du réseau causerait aux entreprises belges. Le rapport de la section opérationnelle rend compte de l'avis de la personne contactée chez *KPNQwest*, décrit l'importance du réseau et les conséquences dommageables que l'arrêt subit du réseau entraînerait pour beaucoup d'entreprises.

- Le 19 juin 2002, le service d'analyse adressa à plusieurs ministres une note décrivant l'intérêt du réseau de *KPNQwest*, et plus particulièrement du réseau *EBONE.* La note fut envoyée aux ministres de la Justice, des Télécommunications, des Affaires économiques, de la Mobilité et des Transports.

- Une énumération des conséquences possibles de l'arrêt du réseau fut présentée : menaces sur la continuité du service aux grandes et aux petites entreprises, perte d'un environnement de haute technologie, perte d'un savoir-faire de haute qualification et perte d'information dans le système. Il fut ainsi mentionné que beaucoup d'entreprises belges – surtout les petites – n'y étaient pas préparées. Par ailleurs, il fut procédé à une énumération des entreprises susceptibles de reprendre l'exploitation du réseau de *KPNQwest*.

- La Sûreté de l'Etat conclut sa note en constatant qu'elle n'est pas, en la circonstance, en état d'évaluer les dommages possibles aux infrastructures vitales du pays et qu'elle doit donc limiter son intervention à cette note d'avertissement.

- La section opérationnelle prit aussi contact avec une responsable de *BELGACOM*, un gros client de *KPNQwest.* Cette personne confirma que le réseau de *KPNQwest* était très performant mais elle déclara que *BELGACOM,* en concertation avec les plus grosses entreprises, avait déjà pris des mesures préventives afin de ne pas subir de conséquences trop dommageables de la faillite de *KPNQwest.*

Par lettre du 19 juin 2002, le chef de cabinet du ministre des Télécommunications a remercié la Sûreté de l'Etat pour son apport dans l'affaire *KPNQwest.* Dans cette lettre, le chef de cabinet fait remarquer :

« In een geliberaliseerde markt is het uiteraard zo dat geen enkele operator kan verplicht worden om zijn dienstverlening verder te zetten, wanneer de economische situatie hem anders doet beslissen. De operatoren zijn vrij hun diensten aan te bieden, maar zijn eveneens vrij hun dienstenaanbod te beperken of stop te zetten op hun eigen initiatief. Inzake het verzekeren van de continuïteit van de dienstverlening, heeft het verleden daarentegen meermaals uitgewezen dat hetzij het volledige netwerk en de desbetreffende individuele vergunning wordt overgenomen door een derde, hetzij het klantenbestand wordt overgenomen door een reeds vergunde operator, hetzij een gedeelte van het netwerk en het klantenbestand wordt overgenomen. Normaliter zal de markt dan ook in een oplossing voorzien voor een dergelijke substantieel netwerk als dat van KPNQwest (…)."

Traduction libre : *« Dans le cadre d'un marché libéralisé, il est évident qu'aucun opérateur ne peut être obligé de poursuivre la fourniture de services si la situation économique lui fait décider le contraire. Les opérateurs sont libres d'offrir leurs services tout comme ils sont libres de limiter leur offre ou de l'interrompre de leur propre initiative. En ce qui concerne la continuité du service, les expériences du passé ont par contre plusieurs fois montré que soit, le réseau est repris dans sa totalité avec la licence individuelle par un tiers, soit la clientèle est reprise par un autre opérateur déjà licencié, soit une partie du réseau et de la clientèle est reprise. Normalement, ce marché devrait trouver une solution pour un réseau aussi substantiel que celui de KPNQwest (…) ».*

Compte tenu de cette réponse et vu le fait que la firme *KPNQwest* venait d'être mise en faillite, la Sûreté de l'Etat décida de clôturer son enquête concernant cette affaire.

4. CONCLUSIONS

Le Comité permanent R constate que, conformément à sa nouvelle mission légale, la Sûreté de l'Etat a manifesté un commencement d'intérêt aux conséquences possibles de la faillite d'une importante entreprise de télécommunication sur le potentiel économique du pays. Toutefois, la Sûreté de l'Etat ne disposait pas encore des moyens nécessaires à évaluer les dommages possibles aux infrastructures vitales du pays et elle dut donc limiter son intervention à une note d'avertissement adressée aux ministres concernés.

La réponse que le ministre des Télécommunications lui a adressée le 19 juin 2002 n'a pas encouragé le service à poursuivre son intervention dans cette affaire.

Le Comité permanent R estime que cette affaire illustre parfaitement la difficulté de définir le rôle que la Sûreté de l'Etat doit jouer dans la protection du potentiel scientifique et économique du pays dans le cadre d'une société fondée sur l'accès ouvert à tous les marchés, la libre entreprise, la mondialisation et la déréglementation.

Le Comité permanent R rappelle par ailleurs que, quatre ans après l'attribution de sa mission de protéger le potentiel scientifique et économique du pays, la Sûreté de l'Etat n'a toujours pas reçu les directives du Comité ministériel définissant les intérêts à protéger ainsi que le prescrit l'article 7, 1° de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Aussi longtemps que ces instructions n'auront pas été élaborées, il n'y a pas lieu d'attendre une implication active de la Sûreté de l'Etat dans ce domaine.

Le Comité permanent R recommande donc une fois de plus que cet obstacle soit levé pour permettre à la Sûreté de l'Etat de remplir sa nouvelle mission.

Il n'entre certainement pas dans l'intention du Comité permanent R de contredire la position du ministre des Télécommunications ; cette affaire concerne en effet un marché libéralisé sur lequel l'autorité a peu d'emprise, ce qui correspond à la conception dominante actuelle en matière économique.

Dans le respect du libre marché, il appartient néanmoins à l'autorité publique de veiller à ce que le potentiel économique et scientifique du pays ne soit pas menacé. C'est précisément à la Sûreté de l'Etat qu'est échue la mission légale d'examiner les dangers et les menaces qui peuvent l'affecter.

Dans un cas comme KPNQwest, ces menaces pourraient par exemple se matérialiser par l'interception de communications, par la perturbation de réseaux de télécommunication (cyber war) ou encore par la prise en main de tels réseaux par des structures maffieuses.

Dans une telle matière, il parait donc recommandable que les ministères des télécommunications et de la Justice puissent collaborer efficacement en échangeant en permanence des informations.

Le Comité permanent R recommande que cette collaboration prenne la forme d'un accord entre le ministère des télécommunications et la Sûreté de l'Etat, possibilité que prévoit explicitement l'article 14 alinéa 2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. En l'occurrence, il reviendrait à la Sûreté de l'Etat de prendre l'initiative en la matière, même en l'absence d'une définition du potentiel scientifique et économique par l'autorité compétente.

CHAPITRE 3: L'ENQUETE DE CONTROLE ET LA PLAINTE CONCERNANT MADAME SOETKIN COLLIER

1. PRISE DE CONNAISSANCE DU PROBLEME ET OUVERTURE DE L'ENQUETE

Le 24 février 2003, le Comité permanent R a reçu une demande du président de la Commission d'accompagnement parlementaire du Sénat visant à diligenter une enquête de contrôle sur la manière dont les informations relatives à Soetkin Collier ont été transmises aux instances officielles et sur la cause des fuites de ces informations dans la presse.

Le 24 février 2003, le Comité permanent R a également reçu une plainte dirigée contre la Sûreté de l'Etat et établie par le conseil de Soetkin Collier avec en annexe une lettre signée par cette dernière.
Dans cette lettre, la plaignante fait référence à un article du journal « *La Dernière Heure* » du 19 février 2003 mentionnant un rapport de la Sûreté de l'Etat relatif à sa personne.

La plaignante déclare que le contenu des informations publiées est inexact, que cette communication constitue une violation du droit fondamental à la protection de la vie privée et que ces informations n'étaient pas exigées par l'intérêt général, de sorte que l'article 19, alinéa 2 de la loi organique des services de renseignement et de sécurité du 30 novembre 1998 a été violé. Elle nie sa présence à la commémoration de Rudolf Hess à Tielrode le 16 août 1996 et elle formule la plus grande réserve quant aux préjudices considérables que les violations précitées ont causés à sa personne.

2. MODALITÉS DE TRAITEMENT

Le Comité permanent R a été chargé, d'une part, d'une demande d'enquête de contrôle sur la manière dont la Sûreté de l'Etat a communiqué les informations aux instances officielles et la vérification de l'origine de la fuite dans la presse et, d'autre part, d'une plainte émanant de Soetkin Collier concernant aussi bien le contenu que le mode de diffusion de ces informations.

Bien qu'il s'agisse en l'occurrence, sur le plan formel, de deux enquêtes distinctes, l'une à la demande du Sénat, l'autre sur la base de la plainte déposée par Madame Soetkin Collier, et que les sujets de ces enquêtes ne sont pas identiques, il va de soi que ces deux enquêtes sont traitées conjointement dans ce rapport parce qu'elles ont pour objet la même problématique.

Le Comité permanent R est donc saisi, sur la base de sa double compétence : d'une part, le contrôle du fonctionnement des services de renseignement, d'autre part, la protection que la Constitution et les lois confèrent aux citoyens à l'égard des activités d'un service de renseignement (article 1 de la loi du 18 juillet 1991 – loi organique des services de police et de renseignement).

Cette double compétence a pour conséquence que les faits concernés doivent être examinés sous différents aspects, d'autant plus que la Sûreté de l'Etat donne plusieurs raisons pour justifier l'envoi de la note litigieuse aux ministres.

Dans le cadre de l'enquête de contrôle, la Sûreté de l'Etat a été entendue, les documents concernés ont été demandés et sur ces bases une discussion spécifique avec des agents de ce service a eu lieu. Pour la suite de l'examen de ce dossier, le Comité permanent R se fonde sur la réponse de la Sûreté de l'Etat du 11 mars 2003 aux questions posées par le Président du Comité permanent R le 28 février 2003.

La plaignante, assistée de son conseil, a été entendue par le Comité permanent R et les éléments apportés par celle-ci ont donné lieu à d'autres actes d'enquête.

3. LES FAITS

Le 9 janvier 2003, la Sûreté de l'Etat a reçu une demande classifiée « CONFIDENTIEL » émanant de la police fédérale de Bruxelles, Service Terrorisme et Sectes, relative à des informations sur une participation au Concours Eurovision de la Chanson 2003.

Dans cette demande, il est fait référence à un article diffusé sur Internet émanant d'un site servant de plate-forme à « een collectief van media-activisten en geëngageerde journalisten» sur lequel un utilisateur de ce site fait allusion à la participation de Soetkin Collier, chanteuse du groupe Urban Trad, au Concours Eurovision de la Chanson 2003. Selon cet article intitulé « La Wallonie envoie une fasciste au Concours Eurovision de la Chanson », Soetkin Collier serait membre depuis plusieurs années de la NSV (nationalistische studentenvereniging) à Gand et d'un « groupement d'extrême droite VRIJBUITER ». Il est demandé si Soetkin Collier est connue de la Sûreté de l'Etat .

Le 9 janvier 2003, la Sûreté de l'Etat prend une décision de déclassification de tous les documents confidentiels et secrets dans lesquels la personne concernée est citée.

Le 14 janvier 2003, la Sûreté de l'Etat transmet à la police fédérale un fax contenant les informations demandées. Ce fax est revêtu du degré de classification « confidentiel » (loi du 11 décembre1998) avec mention de la circulaire qui limite l'utilisation du document (Col. 13/99 – Collège des procureurs généraux).

Dans ce fax, les renseignements disponibles relatifs aux activités de Soetkin Collier concernant plusieurs groupements d'extrême droite, durant la période du 11 novembre 1993 au 30 avril 1998, sont portés à la connaissance du destinataire.

Les mêmes informations sont transmises au Premier ministre, au ministre de la Justice et au ministre des Arts et des Lettres et du Secteur audiovisuel de la Communauté française, par une note non classifiée du 12 février 2003 émanant de la Sûreté de l'Etat .

Sous l'intitulé : « *Participation d'extrême droite belge au concours Eurovision de la Chanson 2003. Cette note reprend des informations au sujet des antécédents d'extrême droite belge de la chanteuse du groupe de music folk « Urban Trac » (sic), que la Belgique enverra au prochain Concours Eurovision de la Chanson qui aura lieu le 24 mai 2003 en Lettonie »,* les éléments suivants sont repris :

- La présence avec une trentaine de manifestants à une action du Voorpost le 11 novembre 1993 perturbant une cérémonie de commémoration du 11 novembre, et au cours de laquelle l'intéressée a été arrêtée administrativement ;

- L'activité de l'intéressée dans la section gantoise de la nationalistische studentenvereniging (NSV) et du Vlaams Nationaal Jeugdverbond (VNJ)

- La détention administrative de l'intéressée pour cause de participation à une manifestation interdite du Taalaktiekomitee (TAK) et du Vlaamse Volksbeweging (VVB) à Wevelgem le 21 février 1996 contre la projection de films francophones au centre culturel local.

- La présence le 16 août 1996 de l'intéressée à une cérémonie de commémoration en l'honneur du dirigeant nazi Rudolf Hess, en compagnie de quelques militants des Vlaamse Jongeren Mechelen (VJM), organisée par le Vlaamse Kring De Dendervrienden à la Vlaamse Herberg à Tielrode (TEMSE).

- La présence de l'intéressée le 30 avril 1998 à un cantus (soirée de chants estudiantins) de la NSV à Gand.

- Les activités de son père, Ivo Collier, ex-militant du VMO et ancien exploitant de l'auberge d'extrême droite « De Leeuw van Vlaanderen » à Anvers.

- En marge des renseignements mentionnés, il est signalé que plus les informations fournies par le site web seront diffusées, plus grande sera la probabilité que des mouvements de protestation soient déclenchés par l'extrême gauche contre la participation de Soetkin Collier au Concours Eurovision de la Chanson.

Le 19 février 2003 et les jours suivants, de nombreux commentaires sont publiés dans les médias relativement aux renseignements communiqués aux différents ministres par la Sûreté de l'Etat et à la décision qui en a résulté de ne pas laisser participer Soetkin Collier à la représentation d'Urban Trad au Concours Eurovision de la Chanson. Sur le site Internet afflue également toute une série de messages avec des points de vue très divers sur cette affaire.

4. ENQUETE SUR LA COLLECTE ET LA DIFFUSION DES INFORMATIONS

Il faut faire une distinction entre la manière dont les informations ont été recueillies, leur mode de traitement et la façon dont elles ont été rapportées.

4.1. La collecte et le traitement des informations

L'article 13 de la loi organique du 30 novembre 1998 stipule que, dans le cadre de leurs missions, les services de renseignement peuvent rechercher, collecter, recevoir et traiter des informations et des données à caractère personnel qui peuvent être utiles à l'exécution de leurs missions et tenir à jour une documentation relative notamment à des événements, à des groupements et à des personnes présentant un intérêt pour l'exécution de leurs missions. Les renseignements contenus dans la documentation doivent présenter un lien avec la finalité du fichier et se limiter aux exigences qui en découlent.

L'article 7, 1° de la loi organique du 30 novembre 1998 stipule que la Sûreté de l'Etat a pour mission : de rechercher, d'analyser et de traiter le renseignement relatif à toutes activités qui menacent ou pourraient 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 ou économique défini par le Comité ministériel, ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Comité ministériel ;

L'article 8 de la loi organique du 30 novembre 1998 stipule que l'on entend par activité qui menace ou pourrait menacer :

c) extrémisme : les conceptions ou les visées racistes, xénophobes, anarchistes, nationalistes, autoritaires ou totalitaires, qu'elles soient à caractère politique, idéologique, confessionnel ou philosophique, contraires, en théorie ou en pratique, aux principes de la démocratie ou des droits de l'homme, au bon fonctionnement des institutions démocratiques ou aux autres fondements de l'Etat de droit .

Il ressort du présent dossier que la Sûreté de l'Etat est restée dans le cadre légal (actuel) relativement à la collecte et au traitement d'informations concernant les associations nationalistes et/ou d'extrême droite citées.

L'intéressée était connue dans les années 1993 à 1998 de la Sûreté de l'Etat, soit parce qu'elle avait été signalée et même arrêtée à l'occasion d'événements au cours desquels elle avait, elle-même, contribué à troubler l'ordre public, soit qu'elle avait été signalée en rapport avec des événements ou en compagnie de personnes en relation avec l'extrémisme.

Même si certaines informations sont contestées (cf. infra), il ne peut y avoir de doute sur le fait que l'intéressée était active durant ces années dans un environnement extrémiste et que la Sûreté de l'Etat a collecté, traité et enregistré à bon droit des informations à ce sujet.

4.2. Le reporting

L'article 19 de la loi organique stipule :

« *Les services de renseignement et de sécurité ne communiquent les renseignements visés à l'article 13, deuxième alinéa, qu'aux ministres et autorités administratives et judiciaires concernés, aux services de police et à toutes les instances et personnes compétentes conformément aux finalités de leurs missions ainsi qu'aux instances et personnes qui font l'objet d'une menace visée aux articles 7 et 11.*
Dans le respect de la vie privée des personnes, et pour autant que l'information du public ou l'intérêt général l'exige, l'administrateur général de la Sûreté de l'Etat et le chef du Service général du Renseignement et de la Sécurité, ou la personne qu'ils désignent chacun, peuvent communiquer des informations à la presse ».

Différentes possibilités peuvent se présenter en regard des dispositions précédentes :

- Il s'agit d'une communication à une autorité ou à un service ; dans ce cas, il existe une double restriction : il doit exister un lien avec les objectifs de la Sûreté de l'Etat et il doit s'agir d'une autorité concernée par l'objet de la menace (comme la Sûreté de l'Etat l'a d'ailleurs elle-même indiqué correctement, les travaux préparatoires de la loi de 1999 indiquent clairement qu'il doit s'agir d'objectifs propres à la Sûreté de l'Etat et non de compétences propres aux autorités alertées).

- Il s'agit d'une communication à une personne qui fait elle-même l'objet d'une menace.

– Il s'agit d'une communication directe à la presse. Dans ce dernier cas, deux conditions sont requises : la vie privée des personnes doit être respectée et l'information du public ou l'intérêt général doit justifier cette communication.

En ce qui concerne cette dernière possibilité, l'enquête exclut toute trace de communication de la Sûreté de l'Etat à la presse. Ce service n'a d'ailleurs jamais eu l'intention de diffuser publiquement une telle note.

L'autre hypothèse selon laquelle il s'agirait d'une personne faisant l'objet d'une menace, n'est pas non plus révélée par les messages initiaux, ni davantage par la justification a posteriori donnée par la Sûreté de l'Etat .

Reste à envisager la communication aux autorités où la question doit être posée de savoir si la Sûreté de l'Etat ne s'est pas trompée dans l'identification de la menace possible.

En effet, rien ne permet de dire que le passé extrémiste de Madame Soetkin Collier constitue en soi et actuellement une menace au sens de la loi précitée. S'il peut être question d'une menace possible, celle-ci résultait peut-être davantage de la manière dont la contestation – fondée sur des informations correctes ou non – relative à la participation de Soetkin Collier a été diffusée sur Internet, et surtout, de l'utilisation future de ces informations lors de l'événement lui-même par des personnes ou des organisations politiques adverses.
Il s'agit d'une hypothèse que la Sûreté de l'Etat mentionne aussi bien dans la note initiale au ministre que dans sa réponse au Comité permanent R, sans que toutefois la nature et la gravité de cette menace ne soient clairement établies.

Il est plausible et même vraisemblable que la participation au Concours Eurovision de la Chanson de Soetkin Collier ait été susceptible de donner lieu à des réactions et même à des actions. Cependant, on ne retrouve nulle part des indications selon lesquelles ces réactions auraient pu constituer à leur tour, et au sens de la loi, une menace réelle.

Le fait de signaler, comme une réponse à la question de la police fédérale, la possibilité d'actions par la transmission d'un rapport nuancé qui aurait replacé le passé de Madame Soetkin Collier dans le contexte actuel, aurait sans doute été légitime en vue de la préservation de la sécurité intérieure et plus particulièrement de celle de l'ordre public.

La Sûreté de l'Etat aurait donc pu se limiter à répondre à la question posée par la police fédérale et laisser toute action ultérieure à l'appréciation de ce service.

Si la Sûreté de l'Etat considérait par ailleurs l'hypothèse de manifestations par des mouvements de gauche comme une menace réelle, il aurait été cohérent que ce service effectue également, au préalable ou ultérieurement, une enquête sur la source de l'information diffusée sur Internet et sur d'éventuels mouvements apparentés ainsi que sur l'objectif et les actions envisagées le cas échéant par ceux-ci. Il ne ressort pas des réponses données par la Sûreté de l'Etat que cette vérification ait été faite.

Il va de soi que ces vérifications auraient également du être effectuées dans le cadre légal de la collecte légitime d'informations et sans mettre en cause le droit à la libre expression de personnes opposées à la participation de Madame Soetkin Collier.

Si par crainte de complications des relations internationales, la Sûreté de l'Etat estimait utile de signaler le passé de l'intéressée suite à sa participation à l'Eurovision - une menace qui serait plutôt de nature symbolique dans le contexte international actuel – ce danger aurait peut-être été davantage circonscrit par une information précise mettant les accents là où il le fallait et encore une fois sous la forme d'un rapport nuancé contenant une évaluation des menaces actuelles. Dans cette hypothèse, il aurait dont été logique que cet élément fût porté à la connaissance du ministre des Affaires étrangères.

Comme la note de la Sûreté de l'Etat a été rédigée indifféremment à destination de divers ministres, le Comité permanent R ne peut y trouver aucune confirmation du fondement légal de sa communication aux autres autorités (à l'exception du ministre de la Justice en tant que responsable direct). En effet, aucune des menaces potentielles, venant soit de Soetkin Collier, soit de la source sur Internet ou d'autres groupements, n'est indiquée qui pourraient se situer dans le cadre de l'application des articles 7 et 11 de la loi organique, puisque ni la sécurité intérieure, ni la sécurité extérieure de l'Etat, ni la pérennité de l'ordre démocratique et constitutionnel, ni davantage les relations internationales ou tout autre intérêt fondamental de l'Etat ne se trouvaient menacés.

4.3. Depuis la classification du rapport, jusqu'à la communication aux ministres et à la « fuite dans la presse »

Bien que la Sûreté de l'Etat ait déclassifié les informations pour permettre leur communication aux ministres, les mêmes informations ont été reclassifiées pour leur communication à la police fédérale.

Etant donné que la réponse de la Sûreté de l'Etat était pourvue de la mention « *confidentiel – Loi du 11 décembre 1998 »* la police fédérale ne pouvait en principe faire usage de ces informations, qu'à des fins judiciaires.

La Sûreté de l'Etat a répondu au Comité permanent R que la reclassification était une erreur.

Dans l'hypothèse ou la Sûreté de l'Etat aurait fait usage de la possibilité de classifier la note aux ministres, une diffusion ultérieure n'aurait, en principe, pas mis en cause la responsabilité de ce service. Dans ce cas, le responsable de la diffusion non autorisée se serait, quant à lui, rendu coupable d'une violation du secret.

Toutefois, lorsque l'on sait qu'en pratique peu de responsables politiques et administratifs disposent de l'habilitation requise pour prendre connaissance d'informations classifiées, la Sûreté de l'Etat se serait quand même rendue coupable d'une violation de la loi sur la classification en transmettant l'information classifiée à une personne non habilitée.

La seule solution aurait sans doute été de conférer au document la mention « Diffusion restreinte ». Cette classification n'est en effet pas assortie de sanctions pénales dans le cas où elle n'est pas respectée. Si elle n'a donc qu'une efficacité limitée quant à la discrétion à garantir au contenu d'un document, elle aurait tout de même eu, dans le cas d'espèce, le mérite d'attirer l'attention des autorités destinataires de la note, sur le caractère sensible des informations.

En tout état de cause, le Comité permanent R constate que la note de la Sûreté de l'Etat est tombée dans le domaine public, de manière telle qu'aussi bien le service que la plaignante ont été l'objet de critiques. Qui plus est, les données de la documentation interne de la Sûreté de l'Etat ainsi que l'identité des agents ayant traité le dossier ont été publiés.

La manière même de faire rapport, indique clairement qu'en l'occurrence la Sûreté de l'Etat n'avait pas l'intention de rendre public – directement ou indirectement – ce document.

L'identification de la personne qui a ultérieurement transmis à la presse la note destinée aux ministres ne ressort pas pour le surplus des compétences matérielles du Comité permanent R.

Une violation éventuelle de la vie privée par méconnaissance des dispositions de l'article 19, alinéa 2 de la loi organique des services de renseignement et de sécurité n'a pas été constatée par le Comité permanent R. En effet, la Sûreté de l'Etat n'a pas fait de communication directe à la presse

4.4. Discussion

La différence de conception entre le Comité permanent R et la Sûreté de l'Etat concernant l'opportunité de la transmission d'informations, comme cela fut fait en l'espèce, ne se révèle pas uniquement importante dans le traitement du présent cas individuel.

L'existence de la Sûreté de l'Etat comme service de renseignements distincts des autres autorités administratives ou judiciaires, répond à une spécificité bien définie.

Cette spécificité implique que la Sûreté de l'Etat consacre son attention à ce qui peut constituer une menace pour l'existence et pour les intérêts de l'Etat et de la population. A cet égard, cette attention doit se porter en premier lieu sur les informations générales qui sont utiles à la prise de décisions de même nature.

Les informations individualisées doivent elles, être traitées et analysées afin de pouvoir donner une image plus précise de la menace générale.

Des informations individualisées peuvent également être mentionnées dans des rapports ou servir de support à l'analyse ou encore être reprises parce que l'aspect individuel constitue en l'espèce l'objet de la communication.

Lorsque le service de renseignement fait lui-même une communication directe à la presse, et que cela peut avoir des conséquences pour une personne déterminée, le service de renseignement doit logiquement, comme l'indique l'article 19, alinéa 2 de la loi organique des services de renseignement et de sécurité, respecter la vie privée, ce qui implique de se conformer à certaines dispositions et procédures.

Bien que la loi n'ait rien prévu spécifiquement, le service de renseignement qui transmet des données à caractère personnel à d'autres autorités, doit faire la balance des intérêts en présence. Ce qui implique parfois de tenter de concilier des points de vue divergents : l'autorité destinataire doit de toute manière être informée de manière correcte et précise (contrairement à un défaut classique des services de renseignement qui, en général, ont parfois tendance à travailler en « circuit fermé », la troisième autorité ne disposant pas alors de toutes les informations nécessaires). Il faut également tenir compte de la protection de ses propres sources, de ses propres agents et méthodes, des enquêtes judiciaires éventuellement en cours, etc … .

Si cela n'est pas exigé par la rencontre d'un intérêt supérieur, le service de renseignement doit également veiller à ne pas exposer inutilement des particuliers à l'attention d'autres autorités, même s'il s'agit de personnes connues pour leur extrémisme actuel ou passé et/ou des personnes de leur entourage.

Cette balance d'intérêts n'est certainement pas une chose aisée et ne devrait pas faire non plus, par la suite l'objet de critiques légères.

La loi organique n'indique pas de quelle manière le service de renseignement doit agir à cet égard. Ce n'est pas non plus nécessaire. Il suffit, en effet, de se référer aux dispositions de la législation spécifique et aux principes d'une bonne administration.

Le Comité permanent R ne souhaite pas approfondir cette question, puisqu'il s'agit également d'une compétence de la Commission de la Protection de la Vie privée et que le président de cette commission est déjà intervenu d'autre part dans ce dossier.

5. LA PLAINTE

La plainte comporte deux éléments :

- d'une part, la contestation de l'exactitude des faits mentionnés dans la note aux ministres et en particulier la présence à une cérémonie à la mémoire de Rudolf Hess qui est niée avec force ;

- d'autre part, la violation de la protection de la vie privée et de l'article 19, alinéa 2 de la loi organique des services de renseignement et de sécurité.

Sur la base du dossier de la Sûreté de l'Etat , il ne peut être établi avec certitude que la plaignante était présente ou non à l'hommage rendu à Rudolf Hess. Les déclarations contenues dans le dossier de la Sûreté de l'Etat et les déclarations de la plaignante devant le Comité permanent R sont, à cet égard, contradictoires.

A l'époque de ses activités dans des milieux extrémistes - où des fractions et des personnes plus ou moins radicales étaient actives, même dans des organisations politiquement structurées - il n'est pas impensable que de telles informations aient été recueillies sur l'intéressée. D'autre part, la plaignante conserve quant à elle le droit le plus absolu de dire qu'il n'en était pas ainsi et d'apporter des éléments qui peuvent infirmer la réalité de cette présence.

Dans le cadre général de la mission spécifique de la Sûreté de l'Etat concernant la collecte d'informations relativement aux activités des organisations d'extrême droite, il n'était pas nécessaire non plus d'obtenir une certitude absolue sur cet élément à charge.

Non pas que les services de renseignement ne sont pas tenus de veiller à cet égard et avec le plus grand soin possible au caractère précis de ces données et à leur éventuelle confirmation, mais bien qu'il ne leur est pas toujours possible, dans le cadre de leurs missions et de leurs moyens, d'amener ces données au même niveau qu'un fait prouvé selon la procédure judiciaire.

Etant donné que des informations individualisées ont été communiquées dans le cas qui nous occupe et que celles-ci constituent l'objet même de la communication, l'exactitude de ces informations revêt une toute autre importance. Il faut constater à cet égard que ces informations proviennent d'une source unique.

Dans la communication aux autres autorités, qui ne sont pas toujours informées des méthodes et circonstances de travail des services de renseignement, il aurait été indiqué de ne communiquer un élément défavorable de cette importance qu'avec la prudence nécessaire ou même, en utilisant le conditionnel.

Les autres renseignements relatifs à la présence à d'autres manifestations ne sont pas niés par la plaignante. Concernant le lien fait par le site web dont question avec le groupe « De Vrijbuiter », aucune activité extrémiste de l'intéressée n'est connue dans la documentation de la Sûreté de l'Etat .

A cet égard, il faut attirer l'attention sur un élément déterminant : il ressort aussi bien de la note de la Sûreté de l'Etat que des déclarations de la plaignante au Comité permanent R, que celle-ci a été remarquée à une activité litigieuse, pour la dernière fois, le 30 avril 1998.

Il s'agit donc, là, d'informations qui datent de plus de cinq ans et qui ne peuvent être complétées par aucune donnée plus récente apportée par la Sûreté de l'Etat. Quelle est donc encore, surtout au vu du jeune âge de la plaignante à l'époque des faits, l'importance de ces informations ?
La plaignante déclare de plus qu'elle a rompu avec l'influence politique que son éducation lui a donnée et elle démontre qu'elle est active depuis lors dans des milieux musicaux qui ne sont certainement pas d'extrême droite et qu'elle donnait cours, en tant que germaniste, à des allochtones.

Concernant le premier élément de la plainte, il faut donc conclure que vu l'individualisation de la notification par la Sûreté de l'Etat, celle-ci est insuffisamment nuancée, en particulier en raison de l'absence d'indication claire de la menace actuelle qu'aurait constitué la plaignante au moment de la transmission de la note.

Concernant le second élément, une violation possible de la vie privée par une méconnaissance des dispositions de l'article 19, alinéa 2 de la loi organique, n'est pas établie par le Comité permanent R étant donné que la Sûreté de l'Etat n'a pas fait de communication directe à la presse (cfr. supra)

Un dernier élément rend difficile, en outre, de se faire une idée exacte de la façon dont ce dossier a été traité. Aucune décision formelle ne semble, en effet, avoir été prise par qui que ce soit, pour demander clairement le retrait de Soetkin Collier. Il s'agit d'une décision « non identifiable » qui a toutefois eu comme conséquence tangible que la plaignante n'a pu participer au festival Eurovision de la chanson. Le Comité permanent R qui n'est pas compétent à ce titre n'estime pas opportun de s'étendre davantage sur cet aspect là du dossier.

6. L'AVIS DU MINISTRE DE LA JUSTICE

En application de l'art. 33 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, le présent rapport a été transmis pour avis au Ministre de la Justice, Monsieur Verwilghen , le 14 mai 2003.

Par courrier du 10 juillet 2003, le Comité permanent R a reçu cet avis, dans lequel le Ministre souscrit à l'analyse de la Sûreté de l'État ainsi conçue :

"(…) De veiligheid van de Staat heeft akte genomen van het rapport van het Vast Comité I betreffende "de wijze waarop de Veiligheid van de Staat informatie - ten laste van een

fysieke persoon en bekend gemaakt via de pers - ingewonnen, geanalyseerd en meegedeeld heeft aan de officiële instanties".

1. Vooreerst dient opgemerkt dat de opvolging en de behandeling van informatie met betrekking tot Mevr. Soetkin COLLIER en de groeperingen waaraan zij kan worden gekoppeld, gebeurden binnen het wettelijk kader met betrekking tot de inlichtingen - en veiligheidsdiensten.

De artikelen 7 en 8 van de wet van de wet van 30 november 1998 belasten de Veiligheid van de Staat, inlichtingen te verzamelen, te analyseren en te behandelen met betrekking tot bepaalde activiteiten die de fundamentele belangen van de rechtstaat aantasten of kunnen aantasten.

Onder deze activiteiten catalogeert de wetgever onder meer de extremistische activiteiten als een bedreiging of mogelijke bedreiging voor de democratische maatschappij.

De in dit dossier verzamelde en behandelde informatie zijn is enkel ingevolge de relatie met het extremisme.

2. De mededeling van de verzamelde inlichtingen met betrekking tot Mevrouw Soetkin COLLIER dient dus gezien binnen dit bestaande wettelijk kader.

Met betrekking hiertoe kan worden gesteld dat de inlichtingenopdracht van de Veiligheid van de Staat zowel een opdracht van verzameling van informatie is als een opdracht om deze mee te delen; de Veiligheid van de Staat heeft dus een informatieplicht zonder dewelke een inlichtingen- en veiligheidsdienst geen enkel nut heeft.

Artikel 19 van de wet van 30 november 1998 is de wettelijke basis voor de mededeling van de inlichtingen. Het is bijgevolg moeilijk vast te stellen in wat de mededeling van inlichtingen door de Veiligheid van de Staat niet zou hebben beantwoord aan het betrokken artikel, gezien de inlichtingen betrekking hadden op extremistische activiteiten.

Dit wordt trouwens bevestigd in het besluit van het Vast Comité I.

3. Wel wordt het actuele belang van de mededeling betwist. De Veiligheid van de Staat heeft evenwel moeten vaststellen dat minstens op de twee websites opgeroepen werd tot reacties tegenover België, gezien Mevrouw Soetkin COLLIER deel uitmaakte van de door België weerhouden deelnemer aan de Eurosong-wedstrijd.

Deze feiten hadden ook de aandacht van de federale politie getrokken.

De objectieve feiten zijn de basis geweest voor de mededeling van de inlichtingen met betrekking tot uitingen van extremisme. De mededeling zelf geeft enkel aan dat de gegevens vermeld in de websites overeenstemmen met inlichtingen waarover de Veiligheid van de Staat beschikte voor de periode van 1994-1998.

De Veiligheid van de Staat is trouwens zeer uitdrukkelijk gesensibiliseerd geworden door de minister van Justitie met betrekking tot het rechts extremisme en dit ingevolge de bespreking in de federale ministerraad van de incidenten met gemeenschapsminister J. SAUWENS (aanwezigheid op een viering van het Sint-Maartensfonds te Antwerpen (Berchem)).

Daarbij komt dat binnen België een gemeenschap aanwezig is die door deze gebeurtenissen ten zeerste zou zijn gesensibiliseerd.

Kortom de Veiligheid van de Staat heeft zich gekweten van haar informatieplicht ingevolge een op dat ogenblik actueel geworden problematiek.

In die context was het niet aan de Veiligheid van de Staat te evalueren of de buitenlandse reactie als dan niet als symbolisch dient (blz. 6 van het rapport) te worden beschouwd.

4. Verder is het voor de Veiligheid van de Staat verrassend te moeten vaststellen dat het Vast Comité I meent dat de Veiligheid van de Staat zich had moeten beperken tot een mededeling aan de Federale politie, die dan verdere actie had kunnen nemen (blz. 6).

De politie treedt op binnen het kader van een strafrechterlijk vergrijp of een bedreiging van de openbare orde. Trouwens, het waren niet de administratieve maar de gerechtelijke onderdelen van de federale politie die optraden, waardoor de hypothese van een onderzoek naar een bedreiging voor de openbare orde hier buiten beschouwing kan worden gelaten.

Het kan toch niet zijn dat de Veiligheid van de Staat haar meer algemene informatieplicht moet opschorten ingevolge een politieoptreden dat normaal gedetermineerd wordt door een stringenter wettelijk kader met veel directere gevolgen voor de betrokken persoon.

Trouwens de instrumenterende politiedienst heeft - van nature - andere gesprekpartners dan de Veiligheid van de Staat. Het kan toch niet zijn dat de Veiligheid van de Staat de naleving van haar wettelijke informatieplicht moet opschorten wanneer een politiedienst - in een niet nader bepaald kader - om informatie vraagt.

5. Het vraagstuk van de opportuniteit van een tussenkomst van de Veiligheid van de Staat, is een vraagstuk dat duidelijk is bepaald door de wetgeving.

Er zijn de reeds eerder vermelde internationale reacties en reacties van gemeenschappen die in bepaalde steden van het land een belangrijke maatschappelijke positie hebben én de invloed die de aanwezigheid van Mevr. Soetkin COLLIER in de deelnemende groep kon hebben op het imago en de naam en faam van België.

Daarnaast, gezien het de deelname van Mevr. Soetkin COLLIER aan een muziekgroep betrof, groep welke dient gezien als een vertegenwoordiger van een belangrijke Belgische niche in die sector en die dus een economische activiteit is, dient er ook in dit kader een bescherming te worden voorzien.

6. De nota van 12 februari 2003 was gericht aan :

- *de Eerste minister, in zijn hoedanigheid van voorzitter van het Ministerieel Comité voor Inlichting en Veiligheid (hij kan in die hoedanigheid beslissen een bepaalde nota te verspreiden bij de leden van dit Comité) én als voorzitter van het overleg van de federale instanties met de gemeenschappen;*

- *de Minister van Justitie, als minister politiek verantwoordelijk voor de Veiligheid van de Staat;*

- *de Minister van de Franse Gemeenschap, onder wiens voogdij de RTBF - als organisator van de deelname van de Belgische groep aan het Eurosongfestival - valt. Het betreft dus de rechtstreeks bevoegde minister.*

Het feit dat het hier gaat om een minister van een gemeenschapsregering, speelt hier geen rol. De wet op de inlichtingen- en veiligheidsdiensten maakt geen onderscheid en spreekt enkel van de bevoegde overheden.

7. De Veiligheid van de Staat stelt vast dat het verslag van het Vast Comité I:

- *stelt dat de Veiligheid van de Staat zijn wettelijke bevoegdheden niet heeft overschreden;*

- *dat het perslek niet het gevolg was van een daad van de Veiligheid van de Staat en er dus geen oorzakelijk verband bestaat tussen de binnen de wettelijke bevoegdheid gestelde daad en de eventuele schade die Mevouw. Soetkin COLLIER zou hebben geleden ingevolge dit perslek.*

De Veiligheid van de Staat nam - hoewel wordt gemeend dat zowel binnen de letter en de geest van de wet werd gehandeld - volgende maatregelen:

- bescherming van de eigen medewerkers door het niet meer vermelden van de namen van de behandelende medewerkers;

- betere juridische kadering van de nota's door het toevoegen van een jurist aan het secretariaat van de adviseur-generaal die er over waakt dat :
  - de wettelijke grondslag van de informatiegaring;
  - de wettelijke grondslag van de mededeling;
  - de wettelijke verplichtingen van de ontvanger,
  uitdrukkelijk voorkomen in de nota's aan de bevoegde autoriteiten.

Tevens zal gevraagd worden aan het Ministerieel Comité voor Inlichting en Veiligheid een duidelijke richtlijn op te stellen met betrekking tot de mededeling van informatie aan de gemeenschappen en gewesten.

Inmiddels zal de Veiligheid van de Staat een brochure uitgeven - voor de politieke beleidsverantwoordelijken en de administraties die nota's ontvangen - met betrekking tot hoe- binnen het huidige wettelijke kader - de documenten van de Veiligheid van de Staat dienen te worden gesitueerd en behandeld. (…)
Koeraad DASSEN, Administrateur-generaal."

7. CONCLUSION

La Sûreté de l'Etat a agi dans le cadre légal (actuel) du recueil et du traitement des informations.

Cependant, le Comité permanent R n'a pu trouver aucune indication démontrant que la participation de Madame Soetkin Collier au festival Eurovision de la chanson pouvait être considérée, à ce moment-là, directement ou indirectement, comme une menace, telle que visée par l'article 7 de la loi organique des services de renseignements et de sécurité

Il n'y avait donc aucune raison de faire rapport à ce sujet aux ministres selon la procédure utilisée, en application de l'article 19, 1er alinéa de la loi organique.

Les informations individualisées concernant Soetkin Collier sont insuffisamment nuancées et ne sont pas accompagnées d'indications permettant d'en faire un usage approprié.

Aucune communication directe n’ayant été faite à la presse par la Sûreté de l'Etat , le Comité permanent R ne peut conclure que ce service a agi en méconnaissance des conditions prescrites par l’article 19, deuxième alinéa.

Le Comité permanent R ne souhaite pas non plus minimiser la responsabilité de la plaignante pour son propre passé, même s’il existe à tout le moins un doute important sur l’exactitude des activités rapportées.

Le Comité permanent R ne prend donc en aucune manière position sur l’adéquation ou non d’exclure la plaignante du concours Eurovision de la chanson.

Principalement, le Comité permanent R regrette toutefois que, dans la chaîne de la transmission des informations ayant abouti à des décisions définitives, la chance n’ait pas été saisie – alors que la possibilité existait – de résoudre ce problème d’une manière conforme aux intérêts de la Sûreté de l'Etat, des responsables politiques et de tous les intéressés.

B. ENQUETES A L'INITIATIVE DU COMITE PERMANENT R

CHAPITRE 1: RAPPORT DU COMITE PERMANENT R SUR LES RESULTATS DE LA TROISIEME PHASE DE L'AUDIT

1. INTRODUCTION ET COURTE SYNTHESE DES RETROACTES

La troisième phase de l'audit de la Sûreté de l'Etat, commencée effectivement la première semaine du mois de novembre 2002 a donné lieu à un rapport rédigé par les experts désignés depuis le début du processus par le Comité permanent R, à savoir Messieurs FRANCEUS, Conseiller général de la Fonction publique et PERREMANS, Directeur au Ministère de la Région wallonne. Ce rapport porte la classification « Secret », pour des raisons évidentes de sécurité.

Le présent rapport, dressé par le Comité permanent R à l'attention des Commissions de suivi parlementaires P et R et de Madame la Vice Première ministre et ministre de la Justice, ne tient compte que des conclusions principales des experts à l'issue de cette troisième phase. Ces conclusions complètent l'éclairage donné par l'ensemble de l'audit sur la manière générale de fonctionner de la Sûreté de l'Etat.

Pour rappel, le Comité permanent R tient à souligner une fois de plus que l'audit a été considéré comme le moyen inévitable de tenter de répondre aux conséquences du climat généralisé d'insatisfaction et de malaise qui existait incontestablement au sein de la Sûreté de l'Etat. Ce climat se manifestait notamment depuis fin 98, par des plaintes individuelles répétées adressées, sous le couvert de l'anonymat, au Comité permanent R[157]. Ce climat a mené à la démission de l'Administrateur général de l'époque, au début de l'été 2002.

L'audit mis en place par le Comité permanent R, avec le soutien conjoint de sa Commission de suivi et du ministre de la Justice de l'époque a certainement contribué à calmer une situation qui, à certain moment, se situait à la limite de l'incontrôlable. L'audit a permis également de réfléchir à l'importance de la fonction d'un service de renseignement, ainsi qu'aux moyens d'améliorer son efficacité et le contrôle de celle-ci, tout en permettant par la même occasion d'assurer une véritable protection des droits et libertés fondamentales des citoyens. L'importance est aussi celle de maintenir des structures indépendantes des forces de police pour accomplir de manière performante les missions décrites par la loi du 30 novembre 1998 organique des services de renseignements et de sécurité, fondamentalement différentes – même si elles sont complémentaires- des finalités policières et judiciaires.

Compte tenu du contexte pré-rappelé, **la première partie de l'Audit** qui s'est déroulée de janvier 2002 au mois de mars 2002, a donc consisté en une enquête d'opinion effectuée auprès de l'ensemble du personnel de la Sûreté de l'Etat. Cette enquête avait pour but d'examiner les facteurs qui, au sein de l'Administration de la Sûreté de l'Etat, contribuaient à motiver ou à démotiver les membres du personnel.

La question fondamentale était donc la suivante : « *L'organisation peut-elle compter sur la motivation de son personnel » ?*

---

[157] Voir notamment : rapport complémentaire d'activités 1999 du Comité permanent R – p.52 et suivantes rapport d'activités 2001 du Comité permanent R – pp. 4,5 et 190, point 2.7

Le Comité permanent R insiste sur le fait qu'il ne s'agissait nullement de s'intéresser à la motivation particulière de chaque membre du personnel pris individuellement, mais bien de donner une évaluation de l'opinion des membres du personnel par rapport à certains éléments objectifs ayant au sein d'une organisation un impact sur la motivation et donc sur l'efficacité du service par rapport à l'ensemble de ses missions légales.

Cette première partie de l'audit devait également permettre de mesurer la volonté de changement du personnel par rapport à ces éléments et de donner aussi une certaine indication des priorités à prendre en considération dans l'avenir.

Dans cette optique, les aspects suivants ont fait l'objet de l'enquête d'opinion :

- La charge de travail et la répartition interne du travail ;
- Le sens donné au travail et les résultats de celui-ci ;
- Les mécanismes de feed-back ;
- L'implication du personnel dans les décisions et la circulation des informations le concernant ;
- La communication interne entre les différents services de la Sûreté de l'Etat ;
- Les perspectives d'avenir et la politique des promotions ;
- La relation de confiance avec la direction et le soutien apporté par celle-ci au personnel ;
- La satisfaction globale.

Sans entrer dans les détails du résultat de cette première partie de l'audit qui a fait l'objet aussi bien d'une information complète et écrite transmise au Ministre de la Justice, Monsieur M. Verwilghen et à la Commission de suivi sénatoriale du Comité permanent R, que de plusieurs échanges de vues avec ces mêmes autorités, il est utile de rappeler ci-après la substance des principales constatations faites à l'époque.

Il faut d'emblée souligner que le taux de réponses à l'enquête a été particulièrement élevé, à savoir, 357 réponses pour 469 questionnaires envoyés, soit un taux de 76% de réponses. Cela démontre, qu'au moment de lancer cette enquête, il existait bien un besoin réel du personnel de la Sûreté de l'Etat de s'exprimer et d'être entendu sur la perception d'une série de problèmes concernant le fonctionnement même de l'institution.

Quant au contenu du message qu'une majorité des participants à cette première partie de l'audit a transmis aux autorités, il témoignait d'une part, d'une perception négative de la relation de confiance entre la hiérarchie et le personnel, de la communication interne et d'une manière générale de la gestion du service. Un aspect positif apparaissait toutefois en rapport avec le contenu du travail, ainsi que dans le désir de voir changer la manière de fonctionner au bénéfice de la Sûreté de l'Etat dans son ensemble.

La seconde phase de l'audit qui s'est déroulée du mois d'avril au mois de juin 2002 a permis d'objectiver les résultats de la première phase.

Le Comité permanent R a trouvé, à ce stade, la confirmation du diagnostic qu'il avait posé à la suite d'enquêtes de contrôle précédentes, selon lesquelles, si la Sûreté de l'Etat recevait bien des signaux en provenances des agents de terrain, ces signaux n'étaient pas toujours – à cause notamment, mais pas uniquement, de déficits structurels – transposés de manière adéquate en analyses pertinentes sur lesquelles les autorités politiques ou judiciaires pouvaient s'appuyer.

La seconde phase de l'audit a confirmé également l'existence d'un malaise au sein du personnel de la Sûreté de l'Etat et en a mis en exergue les causes principales :

- Une absence de management des ressources humaines et un déficit important en communication interne ;

- Une insuffisance de la politique stratégique à laquelle s'est substitué parfois un système rigide et excessif de contrôles administratifs assortis de mesures disciplinaires.

Il apparaissait ainsi qu'un tel contexte avait engendré des comportements négatifs et bureaucratiques privilégiant l'accomplissement de formalités administratives au détriment des missions essentielles du service, principalement le travail de renseignement.

D'une manière fonctionnelle, des insuffisances ont été constatées, dont les plus importantes étaient :

- Un désinvestissement au niveau du cadre du personnel des services extérieurs au cours des dernières années ;

- L'impact négatif de la charge de travail de la section « protection » au détriment des missions de renseignement (la question se posait de savoir si une telle fonction gratifiante au niveau de l'image de la Sûreté de l'Etat était bien une mission d'un service de renseignement);

- L'engorgement structurel des informations au niveau de la direction opérationnelle dans le cycle de transmission du renseignement ;

- La sous-évaluation de l'utilité de la section des « sources ouvertes » et sa position accessoire dans la structure ;

- L'absence d'une bonne collaboration réciproque entre les diverses sections sur la base d'une vision stratégique dont la mise en œuvre demande la participation de toutes les parties concernées.

En marge du rapport de cette deuxième partie de l'audit, il faut rappeler l'importance de la constatation par les experts et par le Comité permanent R, de la compétence et de l'ardeur au travail d'un grand nombre de membres du personnel.

Il avait été constaté également que la participation à l'enquête pour la seconde phase de l'audit était inversement proportionnelle au degré de proximité par rapport à la direction.
Il n'y a pas eu d'explication claire de ce phénomène, mais on peut penser que la démotivation et l'absence d'espoir dans des possibilités de changement étaient plus fortes à mesure que l'on se rapprochait de la direction, un effet d'Icare en quelque sorte.

Les constatations ainsi résumées ci-dessus ont amené à se poser la question sur ce qui devait être fait. Les rapports de l'audit constituaient à ce titre une base pour permettre aux responsables politiques et administratifs d'apporter certaines corrections.

Le Comité permanent R plaidait cependant pour que ces changements ne soient pas apportés sans autre concertation. Un problème peut, en effet, être résolu de diverses manières. Pour de nombreux aspects, il y a de multiples causes à mettre en évidence et, il y a donc des solutions à rechercher dans de multiples domaines.

Par exemple, le fait que beaucoup de chefs de section des services extérieurs devaient s'impliquer de manière excessive dans des formalités administratives de contrôle des présences, constituait un problème qui pouvait être réglé à plusieurs niveaux.

Il est certain qu'un meilleur climat de confiance et de responsabilisation devait être établi, mais on pouvait également envisager d'apporter un soutien administratif à ces responsables de section ou encore adapter le statut pour que les membres des services extérieurs puissent, à un certain âge, se voir attribuer des missions plus administratives ou que des membres des services intérieurs puissent facilement être déplacés vers les services extérieurs.

Cet exemple montre aussi que tous les problèmes ne peuvent pas être résolus uniquement par le remplacement du plus haut fonctionnaire de ce service.

2. LA TROISIEME PHASE DE L'AUDIT

Cette dernière phase a pris un certain retard à la suite de la démission, fin juin 2002, de Madame G.Timmermans, administrateur général et de la nomination, en septembre 2002, de son successeur, Monsieur K. Dassen.

Dès le début 2003, la troisième étape de l'audit a été progressivement relancée après plusieurs échanges de vue avec le nouvel administrateur général de la Sûreté de l'Etat.
Ces échanges de vue et des réunions préparatoires, avec l'assistance des experts, se sont tenus le 13 septembre 2002, le 30 novembre 2002, les 9, 13 et 20 décembre 2002 et le 6 janvier 2003.

Le rapport des experts est classifié « secret » pour des raisons évidentes de sécurité. La présente synthèse classifiée « Diffusion restreinte » de ce rapport, a été approuvée par le Comité permanent R au cours de sa réunion plénière du 19 septembre 2003.

Les principaux éléments, constatations et conclusions de cette troisième phase, sont repris ci-après.

2.1. Objectif de la troisième phase

Il convient de rappeler que le cycle du renseignement comporte trois grandes étapes :

- le recueil des informations ;
- leur traitement ou analyse ;
- la diffusion, classifiée ou non, du renseignement ainsi obtenu

Ces fonctions, dont les deux premières sont internes, doivent être assurées par la Sûreté de l'Etat en conformité avec le prescrit de la loi organique des services de renseignement et de sécurité du 30 novembre 1998. L'information est donc la matière première d'un processus de transformation et d'enrichissement qui conduit à la production du renseignement relatif aux menaces actuelles ou potentielles visées par les articles 7 et 8 de la loi organique précitée.

Ces renseignements doivent à leur tour être diffusés aux autorités décisionnelles responsables qu'elles soient politiques, judiciaires ou administratives. Le recueil et le traitement de l'information relèvent aussi de l'échange entre services de renseignement de différents pays.

La manière dont l'information circule au sein de la Sûreté de l'Etat pour y être traitée est un des aspects importants qui conditionne structurellement l'efficacité de cette administration.

La troisième phase de l'audit avait donc pour objectif – sans s'attacher à l'aspect concret de chaque sujet traité par la Sûreté de l'Etat - de mesurer de façon méthodique *l'efficience* de la diffusion de l'information au sein de l'institution en partant du document de travail de base qu'est le rapport produit par un agent des services extérieurs (il faut souligner que l'audit n'a pas pris en compte les informations venant de services étrangers). Il ne s'agissait pas non plus d'étudier la valeur du système informatique, mais bien la manière dont les acteurs utilisent ce système, au moyen de procédures de travail, d'habitudes culturelles et de réflexes intellectuels. Enfin, cette troisième phase n'avait pas non plus pour objectif d'analyser le contenu des productions de la Sûreté de l'Etat et les effets politiques et sociétaux du travail de cette administration. Ce dernier aspect constitue une des missions légales du contrôle permanent des services de renseignement et s'appréhende par la réalisation, au cas par cas, d'enquêtes de contrôle.

La méthode choisie a été d'exploiter de manière synthétique l'historique des flux, tel qu'il est enregistré dans la base de données adjointe au logiciel de gestion documentaire. A partir du moment où un rapport est introduit dans le système par un agent des services extérieurs, le chemin parcouru par ce rapport est systématiquement enregistré. Cet enregistrement permet de conserver, pour chaque étape du processus, le service traitant, la date et l'heure d'entrée et de sortie, ainsi que les actions manuelles éventuellement appliquées au rapport. Il est important de souligner qu'en fonction du type et du sujet du rapport, le "workflow" a été préprogrammé. Autrement dit, *dans la majorité des cas*, le passage d'une étape à la suivante – le "routage" - se fait automatiquement, étant entendu qu'il est toujours possible de faire intervenir manuellement des acteurs non prévus dans ce flux préprogrammé.

2.2. Le circuit de l'information au sein de la Sûreté de l'Etat

Afin de mesurer l'efficience recherchée, l'exploitation des données récoltées au cours de la troisième phase de l'audit a consisté à évaluer et à mettre en corrélation quatre paramètres liés au processus de traitement de l'information:

- les **quantités** (ou volumes) de rapports introduits et traités;
- les **mouvements**, c'est à dire les passages d'une étape à l'autre (et donc le nombre d'acteurs intervenant dans le traitement de l'information);
- les **destinations** croisées des mouvements "manuels", tenant compte de la répartition (en %) entre les mouvements manuels et préprogrammés.
- les **durées** (de parcours et de traitement).

2.2.1. Quantités

Le nombre de rapports produits par les services de la Sûreté de l'Etat est impressionnant: : plusieurs dizaines par jour. Cette quantité limite leur accessibilité et rend nécessaire une gestion efficace de la connaissance.

La répartition de l'origine des rapports par service et dans le temps ne montre rien d'anormal: il y a une relative proportionnalité - logique - entre l'importance du service en effectif et le nombre de rapports produits et les quelques situations où ce n'est pas le cas, sont explicables par la nature des matières traitées et aussi par l'actualité du sujet concerné.

2.2.2. Mouvements

En moyenne, chaque rapport fait l'objet de 14,6 mouvements. 20% des rapports font l'objet de plus de 16 mouvements.

Certaines matières bien déterminées sont d'office sujettes à plus d'étapes que d'autres.

Pour chaque rapport, 12 acteurs interviennent en moyenne dans le processus. Tenant compte du fait que 10% des mouvements sont des doubles passages dans le même service, ce qui est surtout le cas à la Direction des Opérations (82% des cas), la question de l'utilité pour le Directeur des opérations de recevoir systématiquement deux fois un même rapport se pose incidemment, même si ce dirigeant délègue une grande partie de cette charge de travail.

Nonobstant cette remarque, les plus importants destinataires sont sans surprise:

- les services d'étude;
- la ligne hiérarchique des services extérieurs, jusque la haute direction de la Sûreté de l'Etat .

L'examen de ces mouvements fait apparaître clairement des points d'engorgement : certains acteurs reçoivent tellement de documents qu'il leur est matériellement difficile de tout consulter sans que cela porte préjudice à l'exécution de leurs missions de direction et de coordination.

Une remarque générale doit être faite aussi sur la relative "passivité" des acteurs d'un tel système "push" où l'information est poussée vers le destinataire. Peu de temps et d'initiative sont laissés à chacun pour aller lui-même rechercher l'information. On peut craindre que cela n'affaiblisse la capacité de l'institution dans l'optimalisation du traitement de l'information.

2.2.3. Destination des transmissions manuelles

A chaque étape la hiérarchie de l'agent traitant peut décider de transmettre un rapport à un destinataire supplémentaire à celui prévu dans le workflow préprogrammé. Cela concerne 32% des mouvements annuels.

La répartition entre les destinataires de ces mouvements manuels est très inégale : en général, la hiérarchie reçoit quasi toute la production de manière automatique, alors que les services extérieurs la reçoivent surtout de manière manuelle. Les services d'étude se situent dans une moyenne de 30% de réception suite à un envoi manuel.

De même, la répartition entre expéditeurs est également fort inégale. Par exemple, le secrétariat du Directeur des opérations, transmet - ce qui est logique- de nombreux rapports manuellement.

La corrélation entre les "envois" manuels et les "réceptions" manuelles permet de mettre en évidence la faible communication qui existe entre certains services de la Sûreté de l'Etat.

Ainsi, les échanges sont importants entre agents d'un même service, entre services extérieurs centraux et services provinciaux (excepté dans quatre matières). On distingue d'ailleurs deux "distributeurs" importants, la direction et le secrétariat des services extérieurs ainsi que le chef des services d'étude.

Par contre, les services d'étude forment un circuit plus fermé. On aurait pu imaginer qu'un tel service utiliserait davantage le système informatisé de gestion des flux d'informations pour stimuler certaines actions et recherches auprès des services extérieurs.

Ces constations peuvent expliquer, en partie, l'impression manifestée par une large majorité des agents de la Sûreté de l'Etat, lors de la première phase de l'audit, de "vivre sur une île".

2.2.4. Durées de parcours

On peut distinguer d'une part le temps nécessaire au parcours entre le producteur du rapport et le destinataire final : *la durée du "workflow"* et d'autre part le temps nécessaire au destinataire final pour clôturer le travail : la *durée de traitement*. On ne connaît évidemment pas le temps consacré à la source par l'agent du service extérieur pour rédiger son rapport depuis la prise de connaissance de l'information.

La durée moyenne du workflow automatisé s'élève à une dizaine de jours, ce qui peut être considéré comme normal vu le nombre d'intervenants. Dans 90 % des cas, la durée est inférieure à 5 jours. L'examen des 10 % restants – dont certains montrent quand même un délai très long - ne donne pas de conclusions généralisables, si ce n'est que le système ne permet pas automatiquement aux gestionnaires de détecter les cas de retard inhabituel (absence de sonnette d'alarme…), ce qui constitue à l'estime des experts et du Comité permanent R un risque important pour un service de renseignement.

La durée moyenne de traitement s'élève quant à elle, à moins de 20 jours, mais avec des pointes atteignant plusieurs mois. 10 % des tâches demandent plus de 50 jours de traitement. Cela paraît normal dans le contexte où ce traitement consiste à prendre en considération les informations du rapport dans le but de les consolider, c'est-à-dire, obtenir le feu vert de la hiérarchie pour permettre la poursuite de la diffusion interne du document.
Les délais trop longs peuvent à nouveau constituer un risque important dans les cas où certains maillons de la chaîne pourraient ne pas « suivre ».

A l'occasion de cette analyse, quelques lacunes du système informatique ont pu être identifiées et communiquées aux responsables.

2.3. Conclusions et recommandations

2.3.1. Gestion documentaire

- Une première recommandation porte sur les possibilités non exploitées du système quant au management des flux. En effet, puisque tous les mouvements sont connus, pourquoi ne pas introduire cette connaissance dans le tableau de bord de gestion de l'administration, en particulier un mécanisme de "sonnette d'alarme" concernant les situations anormales de retard. Hormis le cas d'une enquête de contrôle sur un sujet ponctuel, il est sans doute difficile de se faire une idée générale de la valeur exacte d'une information qui arrive à temps auprès d'un destinataire déterminé, de la même manière qu'il est tout aussi difficile d'évaluer la perte d'intérêt d'une information qui arrive trop tard. On peut toutefois sans aucun doute se poser la question de savoir si le système actuel de la Sûreté est apte à éviter les risques inhérents à des messages tardifs. De nouveaux instruments de gestion doivent être développés pour permettre aux expéditeurs des messages et à la hiérarchie de suivre le processus de réponse aux tâches à effectuer.

- Une deuxième recommandation consolidant la première serait de développer davantage des données pour permettre au système d'émarger les rapports d'une mention, du type par exemple de : « (très) urgent » « attention important » ou « routine » (NB : un tel système existe déjà e.a. pour les telex (flash), mais dans la pratique ne préfère-t-on pas utiliser le téléphone ?)

- Concernant l'exploitation même de la base de données documentaires, une suggestion serait d'envisager une meilleure exploitation de la connaissance des informations en procédant à des classifications de celles-ci selon des éléments se rapportant davantage à leurs significations qu'à leur recherche formelle. Ainsi, les documents seraient également « interprétables » au lieu d'être simplement « recherchables ». Dans la même direction, on devrait réfléchir à de nouvelles manières de diffuser l'information sur le plan interne, de façon complémentaire au système existant du workflow et de la base de données. On peut penser par exemple à des forums sur lesquels l'information pourrait être disponible d'une manière plus structurée et plus librement consultable. Cela permettrait des échanges de vue sur des sujets particuliers, échanges de vues qui constitueraient une source importante d'informations tout en améliorant la communication interne. Celle-ci était en effet déficitaire comme cela ressortait déjà de la première phase de l'audit.

- Bien que le système informatique de la Sûreté de l'Etat contienne tous les éléments nécessaires, les statistiques annuelles sont limitées jusqu'à ce jour, à une simple statistique descriptive. A ce sujet et incidemment, il a déjà été indiqué dans la seconde phase de l'audit que, nonobstant l'implication et le professionnalisme des personnes des services informatiques, leur nombre devrait être accru de manière significative. Le recours à des entreprises extérieures n'apparaît pas, quant à elle, le plus indiqué pour des raisons évidentes de sécurité (de surcroît, il est apparu au cours de la 3ème phase de l'audit qu'une information incomplète donnée par une firme extérieure relative à la description d'un modèle de base de données n'était pas de nature à susciter la confiance). En tout état de cause, un système statistique plus élaboré devrait être envisagé qui puisse fonder une gestion stratégique de l'information.

- L'automatisation systématique tend à déresponsabiliser les utilisateurs en les rendant relativement passifs dans le processus et trop confiants dans la technologie. Sans remettre en question cette manière de procéder, qui a certes son efficacité, il faut être conscient qu'elle peut avoir des conséquences négatives quant à la motivation des personnes et l'intérêt qu'elles sont amenées à porter à leur travail. Ce type de système rend également les acteurs moins vigilants. Il est donc recommandé de réfléchir à des mesures qui limiteraient le nombre de mouvements et de tâches à effectuer. Cette limitation dégagerait du temps libre pour un suivi plus actif soutenu par le système informatique.

2.4. Fonctionnement de l'administration

- On peut affirmer, que du point de vue strict de la capacité de rendement quantitatif du service, l'audit a montré que la Sûreté de l'Etat était performante. Par exemple, il y a peu de pertes d'information et globalement le nombre de rapports, d'études et de notes transmises à l'autorité, correspond aux moyens – notamment en personnel - mis à la disposition de l'administration.

- Le décloisonnement interne de la Sûreté de l'Etat est à améliorer, que ce soit du point de vue du transfert de l'information formelle, comme l'a montré cette phase 3, que du point de vue de l'échange de connaissances non formelles, comme l'ont montré les interviews réalisées entre les phases 1 et 2. Le "feed-back" notamment, n'est organisé que sur demande. Les deux boucles de circulation documentaire de l'information et du renseignement (l'une ressortissant des services extérieurs et l'autre des services d'étude) interagissent peu entre elles, sauf à l'endroit du goulot central que constitue le secrétariat des services extérieurs (Direction des opérations - voir ci-dessous). Compte tenu de leur situation centrale et de leur concentration, ainsi que de leur organisation par matière, les services extérieurs de Bruxelles sont toutefois mieux intégrés dans le flux d'informations que les services extérieurs de province. Quoiqu'il en soit, l'existence de ces deux circuits d'informations (services extérieurs et services d'étude) ne présentant que relativement peu d'interactions rend une stratégie globale de l'information très difficile.

- Vu le très grand nombre de documents à traiter, le secrétariat de la Direction des opérations doit nécessairement se limiter à un contrôle formel et de légalité. Cette situation est sans doute illustrée par la constatation que si - via le système du « workflow » - le Directeur des opérations reçoit automatiquement tous les rapports, et parfois même à deux reprises, il ne transmet des ordres concernant des tâches à effectuer qu'à concurrence de 2% (ou 4 % si on tient compte des doubles emplois). Sans aucun doute, il doit y avoir encore d'autres interventions, mais elles ne sont pas comptabilisées dans le système et il est donc impossible d'en connaître la nature ou les caractéristiques de manière non équivoque. En tout état de cause, si comme cela ressortait déjà des phases précédentes de l'audit, on peut conclure que l'intervention du secrétariat des services extérieurs (Direction des opérations) est surtout légitimement et nécessairement axée sur un contrôle formel et de légalité, les experts et le Comité permanent R estiment toutefois que cela ne peut être considéré comme suffisant. On trouve ici quelque part l'écho de ce qui se trouvait déjà mentionné comme une des conclusions importantes de la phase 2 de l'audit : *« Les phénomènes décrits… laissent bien supposer que la direction stratégique constitue un des éléments clés de la Sûreté de l'Etat. Lorsque cette direction diminue peu à peu, on obtient des organisations plus bureaucratiques dans lesquelles la commande est remplacée par du contrôle, où il y a moins d'implication de la base et où la communication est le plus souvent déficitaire….La direction de l'organisation constitue donc la question centrale pour la Sûreté de l'Etat »*

– A rapprocher également de la constatation précédente, le fait que le système actuel de Workflow de la Sûreté de l'Etat crée des doubles emplois injustifiés. Cela indique aussi que l'organisation est surchargée par une affluence de messages et que celle-ci contribue à rendre plus difficile encore le maintien d'une vision globale des divers courants d'information et donc une gestion stratégique. Cela ramène à une recommandation faite in fine du rapport de la phase 2 de l'audit, concernant la structure de la direction de la Sûreté de l'Etat : « …*on devrait pouvoir construire une structure de commande, partant des services extérieurs en collaboration avec les services d'études et les autres services centraux, qui posséderait au moins trois lignes :*

Une première ligne stratégique qui déterminerait ce que la Sûreté aura comme terrain d'action en se basant sur les décisions du Comité ministériel et du Collège du renseignement ;

Une deuxième ligne opérationnelle qui se pencherait sur la réalisation de l'activité (méthodes de travail, normes…) ;

Une troisième ligne logistique déterminerait les moyens de toute nature, utiles et à utiliser pour réaliser la mission.

Le sommet de la hiérarchie devrait intégrer et harmoniser cela et en prendre le contrôle à son propre compte tout en insistant sur la participation »

En tenant compte des résultats de la troisième phase de l'audit, le Comité permanent R reprend ces suggestions, dans le sens où la tâche de déterminer une ligne stratégique doit aussi s'entendre au sein de la Sûreté de l'Etat comme la mise en carte de la stratégie du flux de l'information, c'est-à-dire, le développement d'une stratégie de l'information, la mise sur pied d'un instrument de suivi et de gestion efficace de la collaboration entre les différents acteurs de la Sûreté de l'Etat et, enfin, la gestion de ces flux d'informations et le suivi actif de cette stratégie de l'information.

2.5. Dernières remarques concernant la notion d'efficacité

Le contrôle de l'efficacité des services de renseignement constitue une des missions permanentes du Comité permanent R. On peut certainement et légitimement penser qu'un des éléments de mesure de cette efficacité se rapporte aux résultats positifs pour la société belge résultant des renseignements produits par la Sûreté de l'Etat. En comparaison avec les moyens mis à la disposition de ce service combien de menaces au sens de la loi organique des services de renseignement ont-elles été détectées et évitées, combien de réseaux criminels ou terroristes identifiés ou démantelés, combien de ressources scientifiques et économiques sauvegardées ?

Auditer une organisation, c'est aussi poser ces questions. Les interviews réalisées au cours de l'audit, ont montré qu'un certain nombre d'acteurs au sein de la Sûreté de l'Etat avaient un point de vue "critique et constructif" sur cette problématique de l'efficacité. Toutefois, la mesure de cette dernière ne peut s'évaluer de manière globale et absolue. Elle nécessite de se pencher à un moment donné sur un sujet spécifique et d'évaluer la qualité du renseignement et son adéquation à l'attente des autorités destinataires ainsi qu'à la politique du renseignement telle qu'elle doit être définie par le Comité ministériel. Ce sont ces différents éléments que le Comité permanent R vise à appréhender dans la réalisation d'enquêtes de contrôles particulières.

L’audit, comme cela a déjà été souligné, avait pour point de départ de rencontrer un malaise général exprimé par le personnel de la Sûreté de l’Etat. Son but principal était donc de répondre à cette manifestation en essayant de mettre en évidence les problèmes structurels qui pouvaient être à la base de l’insatisfaction quasi générale, étant bien entendu que ceux-ci ne pouvaient qu’avoir des conséquences négatives sur l’efficacité du service. Ce sont ces éléments structurels qui ont été évalués dans le cadre des 3 parties de l’audit : le personnel, l’organisation et enfin l’information. Le Comité permanent R estime donc que la troisième phase ainsi achevée clôture la procédure d’audit sensu stricto.

Les constatations faites qui se sont confirmées et consolidées au cours des trois périodes successives du travail des experts sont à prendre en compte par la nouvelle administration générale de la Sûreté de l'Etat dans le cadre des réformes internes qu’elle a déjà initiées, et dont le Comité permanent R suivra l’évolution dans le cadre de sa mission de contrôle.

L’audit a permis au Comité permanent R d’avoir une meilleure compréhension générale du fonctionnement réel de la Sûreté de l'Etat. Cette vision lui permettra de mieux replacer certains problèmes plus particuliers dans leur contexte.

Il est évident, en effet, que de nombreuses questions en relation avec l’efficacité d’un service de renseignement doivent encore faire l’objet d’évaluations attentives tant sur le plan de l’amélioration éventuelle de celle-ci que sur celui de la protection proportionnelle des libertés et droits individuels de la personne face à un service de renseignement équipé de systèmes informatisés extrêmement puissants. Ces questions relèvent de l’accomplissement des missions légales du Comité permanent R.

Certains des aspects de cette efficacité, comme la communication de renseignements à destination des diverses autorités nationales et internationales fait d’ailleurs déjà l’objet, de manière ciblée ou générale, d’enquêtes de contrôle en cours.

Les résultats de celles-ci seront communiqués, dès leur achèvement, dans des rapports distincts à Madame la Vice Première ministre et ministre de la Justice et à la Commission de suivi du Comité permanent R.

CHAPITRE 2: RAPPORT D'ENQUETE SUR L'EFFICACITÉ DE LA SECTION DE PROTECTION DES PERSONNES DE LA SURETE DE L'ETAT A PROPOS D'UN INCIDENT DE SECURITE SURVENU DURANT UNE MISSION

1. ANTECEDENTS ET OUVERTURE DE L'ENQUETE

L'enquête a été ouverte d'initiative par le Comité permanent R.

Les autorités parlementaires et politiques ont été averties les 29 et 30 mai 2001.

Les motifs de cette enquête trouvent leur origine dans la préoccupation du Comité permanent R relative à d'éventuels incidents qui pouvaient se produire au cours de l'année de la présidence belge de l'Union européenne. Au cours de celle-ci, en effet, de nombreuses visites formelles et informelles, ainsi que des réunions de représentants étrangers de haut niveau, susceptibles de faire l'objet d'une protection rapprochée (« close protection ») de la part de la section « Protection» de la Sûreté de l'Etat devaient avoir lieu.

Cette préoccupation ne reposait certes pas sur des indications que le personnel de cette section n'était pas adapté ou compétent, mais sur l'ampleur et la fréquence des missions et le climat de plus en plus tendu faisant suite aux sommets précédents riches en incidents.
Le Comité permanent R craignait, compte tenu de ces derniers éléments, que la section éprouve des difficultés à mener, à bonne fin, ces très importantes missions. C'est d'ailleurs aussi, dans un contexte similaire, que se situe une autre enquête de contrôle du Comité permanent R sur le suivi par la Sûreté de l'Etat du phénomène anti-mondialiste.

Un incident survenu le 5 mars 2001 lors de la mission de protection du Président Mugabe du Zimbabwe, exécutée par les membres de la Sûreté de l'Etat, a été l'élément concret qui a, dans ce contexte, contribué à motiver la présente enquête.

A cette occasion, un opposant non armé du Président Mugabe fut violemment pris à partie par le service de sécurité de ce chef d'Etat. Ces faits, tels que diffusés à la télévision, faisaient suite à un autre programme de RTL dans lequel on faisait l'éloge de la section «Protection» de la Sûreté de l'Etat.

Le Comité permanent R estima donc opportun de se forger un jugement indépendant sur l'efficacité de ce service en partant d'un incident concret.

L'existence d'autres priorités ont justifié que le rapport du Service d'enquêtes remis le 13 juin 2001 au Comité permanent R ne fut pas immédiatement exploité dans le cadre d'un rapport final.

Le Comité permanent R estime néanmoins que l'enquête menée sur un incident déjà ancien, ne peut rester sans suite, compte tenu de ses éventuelles implications au niveau des principes et acheva celle-ci en approuvant le présent rapport le 6 mai 2003.

2. L'ENQUETE CONCERNANT L'INCIDENT

L'incident est survenu dans le cadre de la visite officielle du Président du Zimbabwe en Belgique. Comme il est d'usage, un visiteur de ce niveau est entouré de diverses mesures de sécurité qui sont confiées à différents services, principalement les services de police, suivant des instructions permanentes et sous la coordination du Ministère de l'Intérieur.

La Sûreté de l'Etat a pour mission de protéger au maximum l'intégrité physique (protection personnelle) du visiteur. Cette mission est exécutée par les membres d'une section spécifique de la Sûreté de l'Etat. Ces fonctionnaires jouissent de compétences particulières inscrites dans la loi du 30 novembre 1998 organique des services renseignements et de sécurité et reçoivent une formation spécifique. Cette mission d'officier de protection est fondamentalement différente de la mission de la plupart des autres membres de ce service de renseignement qui s'occupent de collecter, de traiter et de transmettre des renseignements.

Souvent, les visiteurs étrangers sont aussi accompagnés par leur propre service de sécurité. La présence d'une protection propre au visiteur étranger est une pratique admise (sous certaines conditions) mais ce service étranger n'a aucune autre compétence que l'accompagnement (armé) du visiteur.

L'incident lui-même consistait en la présence dans un hôtel bruxellois où séjournait le président du Zimbabwe, d'un sujet britannique opposé à sa politique et à son régime notamment en ce qui concerne la répression des homosexuels. Lors d'un départ de l'hôtel du Président Mugabe, cet opposant manifesta son opposition. D'après les médias britanniques, il aurait même tenté d'arrêter Mugabe en tant que citoyen (citizen's arrest) pour cause de violation de la Convention contre la torture.

Dans la confusion qui s'en suivit, le manifestant fut repoussé sans violence par un membre de la Sûreté de l'Etat, alors que le Président était évacué vers son véhicule blindé. Par la suite, l'opposant aurait été molesté par la protection personnelle (garde du corps) du Président. Les membres de la section « Protection» de la Sûreté de l'Etat ont constaté cela de visu.

D'une manière générale, il faut souligner que, la Sûreté de l'Etat ne disposait pas d'indices de menaces contre la personne du Président Mugabe.

Le manifestant était à nouveau présent quelques instants plus tard au domicile de fonction du Premier ministre, qui recevait le chef d'Etat Zimbabwéen, mais il fut maintenu à distance par la police sur instruction de la Sûreté de l'Etat. En même temps, le chef de la sûreté étrangère fut sommé de ne pas outrepasser ses compétences.

3. EVALUATION DE L'INCIDENT

Pour autant qu'il pouvait être évité, l'incident n'était pas imputable à une erreur manifeste des membres de la Sûreté de l'Etat qui ont bien rempli leur mission principale qui consistait à protéger un visiteur officiel.

La Sûreté de l'Etat ne doit pas tenir compte pour cela de la politique menée par la personnalité en question ni des opinions des manifestants, si ce n'est comme indication du risque potentiel.

Il était sans doute possible d'éviter ou de limiter l'incident, qui doit plutôt être qualifié de trouble de l'ordre public, par une meilleure information préalable de l'équipe de la Sûreté de l'Etat et/ou un meilleur encadrement par le service de sécurité de l'hôtel ou de la police locale.

Il y a, en effet, des indices selon lesquels les services de sécurité de l'hôtel, le service de sécurité Zimbabwéen et même la Sûreté de l'Etat avaient été informés peu auparavant d'un « possible incident médiatique ». Il fut certainement demandé à la Sûreté de l'Etat d'utiliser une autre sortie. Apparemment, cela n'a pu se faire par manque de temps ou d'information suffisante.

Vu l'issue relativement bénigne – même si l'incident eu quelques conséquences diplomatiques parce que les autorités britanniques ne pouvaient tolérer le traitement réservé à leur sujet – le Comité permanent R n'a pas estimé opportun de procéder à une enquête plus ciblée, étant donné notamment que des personnes impliquées au premier chef ne résident plus dans le pays.

Le cas d'espèce démontre, en tout cas, que des incidents d'ordres divers, dirigés ou non contre la sécurité des VIP, ne peuvent pas toujours être évités, soit parce que « l'agresseur » (verbal dans ce cas) n'est pas intimidé par le dispositif de sécurité ou parce que le service de sécurité étranger ne s'en tient pas aux règles établies ou encore parce que, comme ici, les deux hypothèses se présentent en même temps. Il va de soi que le service de sécurité étranger n'avait pas le droit de maltraiter un manifestant.

L'événement qui a été filmé sert, en tout cas aujourd'hui comme cas pratique, pour la formation des membres du service de protection.

4. EVALUATION GENERALE

Le Comité permanent R ne voit pas dans cet incident une raison de mettre en cause la Sûreté de l'Etat . Le Comité permanent R est parfaitement conscient du fait que la différence entre un palmarès irréprochable et une mauvaise réputation internationale dépend parfois d'un détail et que l'erreur la plus minime, diffusée à l'envi par les médias, peut être utilisée en vue de discréditer tout un service après-coup.

On doit toutefois regretter pour des raisons de principe que la Sûreté de l'Etat n'ait pas dénoncé d'office aux autorités judiciaires les coups portés au manifestant.

De manière générale, il n'y a aucun reproche à faire à cette section de la Sûreté de l'Etat.

Si le Comité permanent R a dû constater quelques dysfonctionnements dans cette section par le passé, ceux-ci portaient sur l'administration des prestations et des rémunérations, et non sur la qualité même du travail de protection.

A l'issue de la présidence belge, le Comité permanent R, tout comme les autres autorités belges, ne peut que féliciter cette section de la Sûreté de l'Etat pour le bon déroulement des missions de protection.

Le Comité permanent R profite de l'occasion pour répéter et préciser ses positions concernant cette mission de la Sûreté de l'Etat.

Tout d'abord, le Comité permanent R ne rencontre aucun problème quant au fait que cette mission, que l'on peut intrinsèquement qualifier de mission de police administrative, soit exercée par la Sûreté de l'Etat .

Cela présente notamment l'avantage que le service peut se positionner vis-à-vis du monde extérieur avec une section qui bénéficie de l'intérêt des médias et qui peut donc servir « d'image de référence », en vue de susciter, par exemple, une vision positive du service qui peut toujours s'avérer utile pour le recrutement de nouveaux agents.

Le Comité permanent R rappelle et précise à cet égard quelques conditions corollaires qui doivent empêcher que cette mission ne porte d'autre part préjudice à la mission principale du service.

Elles concernent principalement l'intégration de membres d'autres sections s'occupant elles de renseignement dans le cadre du personnel du service de protection. Lors de la mission qui nous intéresse, et étant donné la surcharge à ce moment des missions de protection simultanées, l'équipe était ainsi majoritairement composée de renforts provenant d'autres sections de la Sûreté de l'Etat .

5. RECOMMANDATIONS

- A la lumière de cet incident, par ailleurs non significatif pour le fonctionnement de la section, le Comité permanent R estime qu'il serait utile de donner des instructions à la section de protection sur les cas où des mesures devraient être prises à l'égard des services de sécurité du VIP. Dans le cas présent, il aurait été opportun de faire immédiatement une dénonciation au parquet en exécution de l'article 29 du Code d'instruction criminelle.

- Le Comité permanent R est d'avis que la section de protection de la Sûreté de l'Etat doit disposer d'un personnel suffisant en vue de faire face à une charge de travail normale (e.a. récupérations, formations, …). Cette section ne peut être renforcée que par du personnel bien formé (p.ex. : anciens membres de cette section), qui ont au moins suivi la formation de base et des recyclages réguliers.

- Le renfort par une affectation temporaire à cette section ne peut porter préjudice au travail de renseignement proprement dit en retirant du personnel d'autres sections.

- Le renfort ne peut consister en membres des services extérieurs qui effectuent du travail de renseignement en tant que tel (comme des agents qui ont des contacts avec des informateurs, effectuent des observations, etc …). En exposant les agents au public (directement ou par l'entremise des médias), ceux-ci sont susceptibles d'être reconnus dans des situations ou cela n'est pas souhaitable, ou même dangereux pour leur mission et, le cas échéant, pour leur sécurité personnelle.

– Le Comité permanent R estime par conséquent que la limite imposée aux services de renseignement, par la loi organique, entre les missions de protections et les missions de renseignement au cours desquelles l'officier de protection exécute cette mission « à l'exclusion de toute autre mission » (article 22), devrait avoir son corollaire dans le sens ou un officier de renseignement ne devrait pas pouvoir effectuer, même d'une manière occasionnelle et alternative, des missions de protection.

CHAPITRE 3: RAPPORT DE L'ENQUÊTE SUR « LA MANIÈRE DONT LES SERVICES DE ENSEIGNEMENT ONT TRAITÉ ET DIFFUSÉ DES INFORMATIONS RELATIVES À DES AFFAIRES DE FRAUDE AUX VISAS ET AUTRES DOCUMENTS FAVORISANT LA TRAITE DES ÊTRES HUMAINS VERS LA BELGIQUE »

1. INTRODUCTION

Tant en Belgique qu'en France et en Italie, la problématique des faux visas et faux documents d'identité pour pouvoir commettre des délits a commencé à être évoquée à partir de l'année 1997. Les passeports belges volés en 1999 et utilisés par les assassins présumés du commandant afghan Massoud le 9 septembre 2001 ainsi que les tragiques attentats aux USA le 11 septembre ont été l'occasion de remettre ce problème sur le tapis.

Le 5 mars 2001, M. Johan Leman, Directeur du *«Centre pour l'égalité des chances et la lutte contre le racisme»* (CECLR), a été entendu par la Sous-commission *«Traite des êtres humains et prostitution»* du Sénat. Il y a évoqué l'affaire des faux visas à l'ambassade de Belgique à Sofia, ainsi que l'octroi de fausses cartes d'identité au service Protocole du ministère des Affaires étrangères.

En juin 2001, l'attention du Comité permanent R a été attirée par le rapport que le CECLR a consacré à la lutte contre la traite des êtres humains.

C'est avec le même intérêt que le Comité permanent R a suivi le colloque *"Maffias et traite des êtres humains"* organisé par le Centre le vendredi 15 juin 2001.

Souhaitant poursuivre son information sur ces sujets, le Comité permanent R s'est entretenu le vendredi 6 juillet 2001 avec M. Johan Leman, Directeur du CECLR.

Le Comité permanent R s'est demandé si la Sûreté de l'Etat avait enquêté sur ces affaires qui semblaient concerner des organisations criminelles liées au trafic des êtres humains, menace dont ce service doit aussi s'occuper aux termes des articles 7 et 8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Dans un premier temps, le Comité a examiné comment la Sûreté de l'Etat avait traité l'affaire des faux visas découverte en 1997 à l'ambassade de Belgique à Sofia ainsi que l'octroi de fausses cartes d'identité par un membre du service Protocole du ministère des Affaires étrangères.

Le Comité permanent R a ensuite examiné de manière plus générale comment la Sûreté de l'Etat et le SGRS appréhendaient la problématique de la délivrance de faux documents, passeports et visas favorisant le trafic d'êtres humains vers la Belgique.

2. PROCÉDURE

Le 9 juillet 2001, les membres du Comité permanent R ont décidé à l'unanimité d'ouvrir une enquête d'initiative *«sur les renseignements dont dispose la Sûreté de l'Etat à propos d'une affaire de fraude aux visas évoquée au Sénat, notamment dans le contexte de la traite des êtres humains».*

Le Président du Sénat en a été averti le 16 juillet 2001 et le Ministre de la Justice, le 18 juillet 2001.

Le Comité permanent R a chargé son Service d'enquêtes de procéder à toute investigation utile auprès de la Sûreté de l'Etat. La plupart des réponses de la Sûreté de l'Etat sont classifiées «SECRET» au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité.

Le Comité a par la suite examiné comment la Sûreté de l'Etat suivait la problématique générale de la traite des êtres humains, notamment dans le sport, matière évoquée au Sénat au cours des années 2002 et 2003 (Rapport parlementaire 2 - 1132/2).

Au mois de juin 2002, la Sous-commission du Sénat *«Traite des êtres humains»* a accepté le principe que Comité permanent R soit associé à ses travaux. Néanmoins, aucune invitation à participer aux réunions de la Sous-commission n'a jamais été adressée au Comité.

Un rapport classifié « CONFIDENTIEL » au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité a été approuvé par le Comité permanent R le 6 mai 2003. Cette classification est justifiée par l'atteinte possible qu'une utilisation inappropriée de ce document pourrait causer à la vie privée de certaines personnes d'une part, au fonctionnement d'organes décisionnels de l'Etat d'autre part.

A la même date, le Comité permanent R a également approuvé la présente version du même rapport, classifiée « CONFIDENTIEL » au sens de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

Ce rapport est destiné à la Commission du Sénat chargée de l'accompagnement du Comité permanent R ainsi qu'aux ministres compétents. Il est confidentiel au sens de l'article 33, alinéa 3 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

Il est revêtu de la mention « DIFFUSION RESTREINTE » en application de l'article 20 de l'arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité.

Ce rapport a été adressé à M. Marc Verwilghen, Ministre de la Justice le 3 juillet 2003 en lui demandant de communiquer son avis sur ce document au Comité permanent R.

Le 6 août 2003, la Sûreté de l'Etat a transmis ses observations sur ce rapport à Madame Laurette Onkelinx, nouvelle Ministre de la Justice.

Au jour de l'approbation du présent rapport, (le 16 mars 2004) le Comité permanent R n'avait encore reçu aucun avis de la part du Ministre sur son rapport.

Ce même rapport fut par ailleurs adressé le 7 octobre 2003 au président à la commission du Sénat chargée de l'accompagnement du Comité permanent R. A la date du 16 mars 2004, ce rapport n'avait pas encore été discuté par cette commission.

Par ailleurs, le Comité permanent R a fait procéder à des devoirs d'enquête complémentaire au cours des mois d'août et de novembre 2003 auprès de la Sûreté de l'Etat. La Ministre de la Justice en a été avertie le 28 août 2003.

Le Comité permanent R a aussi décidé au cours du mois d'août 2003 d'étendre son enquête au SGRS afin de savoir si ce service avait également connaissance de l'existence de systèmes de délivrance de faux visas, passeports ou autres documents d'identité belges dans certaines ambassades de Belgique à l'étranger et, dans l'affirmative, comment il traitait cette matière.

Le ministre de la Défense nationale été avisé de cette décision le 6 août 2003.

La plupart des réponses et documents obtenus de la Sûreté de l'Etat et du SGRS sont classifiés « confidentiel» voire « secret » au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité.

Le Service d'enquêtes R a produit quatre rapports complémentaires qu'il a respectivement adressés au Comité le 3 septembre 2003, le 12 décembre 2003, le 21 janvier 2004 et le 4 février 2004.

Le présent rapport, approuvé le 16 mars 2004, constitue une mise à jour du premier rapport approuvé le 6 mai 2003. A cette occasion, le Comité permanent a décidé de renommer son enquête de la manière suivante « *enquête sur la manière dont les services de renseignement ont traité et diffusé des informations relatives à des affaires de fraude aux visas et autres documents favorisant la traite des êtres humains vers la Belgique* » .

3. CONSTATATIONS

3.1. La Sûreté de l'Etat

3.1.1. La manière dont la Sûreté de l'État s'occupe de la traite des êtres humains en général

A la question de savoir si la Sûreté de l'Etat suivait la problématique de la traite des êtres humains d'une manière générale, ce service répond [158]:

« Le gouvernement a placé le problème de la traite des êtres humains parmi ses priorités. Ceci appert d'ailleurs du plan fédéral de sécurité. C'est à la demande expresse du gouvernement que la Sûreté de l'Etat suit cette matière.

[158] Traduction libre

Au sein de notre service, la traite des êtres humains est étudiée en tant que composante du crime organisé. En fonction des peines prévues et des risques d'être pris, les groupes organisés de ce milieu exercent alternativement leurs activités dans le trafic de drogues ou de voitures ainsi que dans le trafic et la traite des êtres humains.

Les fonds que génèrent ces activités sont destinés à s'acheter une conduite dans le monde « normal ». Nous pensons notamment à cet égard à l'acquisition de biens immobiliers, de participations dans des entreprises et aux prises d'intérêts dans les milieux sportifs. Ayant acquis de la sorte une certaine position sociale, ils sont à même d'exercer certaines influences au niveau politique et du monde des affaires.

C'est précisément parce que la traite des êtres humains est considérée comme un élément du crime organisé que, lors de la mise en carte des réseaux qui se dissimulent derrière la traite des êtres humains et l'immigration illégale, l'on suit la même méthodologie que celle utilisée pour nos enquêtes relatives au crime organisé. D'ailleurs l'expérience antérieure acquise pour les groupes extrémistes et terroristes où les mêmes méthodes ont été employées joue au niveau de la traite des êtres humains.

Il en résulte que l'information dont la Sûreté de l'Etat dispose dans le cadre de la traite des êtres humains provient de sources ouvertes (Internet, conférences, etc.), d'instances officielles, de correspondants étrangers et d'informateurs.

Notre service reçoit de ces diverses sources des informations concernant l'immigration illégale, le trafic et la traite des êtres humains.

Elles peuvent porter plus spécifiquement sur :

- les facteurs qui déclenchent l'immigration illégale ;
- le profil des réfugiés/victimes ;
- les techniques utilisées (y compris l'usage illégal de documents et de procédures officielles) ;
- les itinéraires suivis ;
- les organisateurs/réseaux ;
- les intermédiaires (y compris les négriers du logement et des avocats peu scrupuleux).

Ces informations sont traitées de manière opérationnelle et analytique et ont, à ce jour, donné lieu à un nombre non négligeable de rapports et d'analyses internes destinés aux autorités judiciaires et administratives».

A la question de savoir si la Sûreté de l'Etat suivait d'une manière ou d'une autre la problématique de la traite des êtres humains dans le sport, ce service répond [159]:

«Le secteur sportif est suivi dans le cadre général du crime organisé. Comme pour tout autre secteur, nous informons les autorités si nous constatons des problèmes ou des abus.»

La Sûreté de l'Etat a effectivement produit plusieurs analyses sur la traite des êtres humains à partir de l'année 2000 qui ont été transmises aux autorités administratives et judiciaires compétentes.

A la question de savoir si la Sûreté de l'Etat participait aux travaux de la Task Force *«Traite des êtres humains»* créée par le gouvernement en décembre 2000, ce service répond [160]:

[159] Traduction libre
[160] Idem

«Pour la mise en œuvre du plan fédéral de sécurité et de politique pénitentiaire en matière de traite des êtres humains et de pornographie enfantine, un groupe de travail présidé par le Service de la politique pénale a été créé. La Task Force «Traite des êtres humains» s'est chargée de créer le Centre d'information et d'analyse «Traite des êtres humains» (CIAT). La Sûreté de l'Etat y a participé.(…)

« (…) Notre service n'a cependant pas attendu que le CIAT devienne opérationnel pour établir et entretenir des contacts avec les services actifs dans la lutte contre la traite des êtres humains. C'est ainsi qu'il existe, dans un cadre bilatéral notamment, une concertation entre notre service et l'Office des étrangers, le Commissariat général aux réfugiés et apatrides, la Cellule «Traite des êtres humains» de la Police fédérale, les Affaires économiques et l'Inspection sociale.

Notre service dispose d'ailleurs d'un officier de liaison à l'Office des étrangers. Cette fonction sera évaluée et éventuellement adaptée dans le cadre du plan de gestion.

Notre service est toutefois convaincu qu'une coopération transfrontalière est indispensable dans le cadre de la lutte contre l'immigration illégale et la traite des êtres humains.

Nous participons à la réunion préparatoire ainsi qu'à la réunion proprement dite du Groupe de travail européen CIREFI (Centre d'Information, de Réflexion et d'Echange d'informations pour le Franchissement des frontières et l'Immigration).

De plus il existe également entre les différents services de renseignement une coopération internationale dans le cadre de laquelle ces informations sont échangées».

Outre les réponses aux questions posées par le Comité permanent R, la Sûreté de l'Etat lui a transmis 147 notes rédigées par ses services d'études à propos de la traite des êtres humains et de l'immigration illégale et qui ont été communiquées aux autorités.

Elles portent sur une période de 3 ans dont la moitié environ, c'est-à-dire quelque 18 mois, a précédé la décision du gouvernement (mi-2001) d'inclure dans ses priorités la lutte contre la traite des êtres humains.

Le Service d'enquêtes R s'est chargé de résumer ces notes. Ceci a notamment permis de faire ressortir le contexte dans lequel les données transmises ont été collectées et comment s'était déroulée la collaboration avec divers services et autorités.

Dans l'ensemble, les notes ont également permis au Comité permanent R d'avoir un bon aperçu de la manière dont la Sûreté de l'Etat a, pendant une période relativement courte (3 ans), fourni aux autorités des données relatives à la matière spécifique, de la traite des êtres humains.

La majorité des notes (90/197) concernaient la communication de faits ou le suivi d'affaires que la Sûreté estimait, dans certaines circonstances, devoir être portés d'urgence à la connaissance des autorités compétentes.

3.1.2. Compétence de la Sûreté de l'État en la matière

Dans une série de notes adressées au cours de l'année 2001 au Premier Ministre, aux Ministres de la Justice, de l'Intérieur et des Affaires étrangères, ainsi qu'au Magistrat national et au Directeur de l'Office des étrangers, la Sûreté décrit de la manière suivante sa mission, son rôle et ses activités en matière de lutte contre la traite des êtres humains.

La loi du 30 novembre 1998 organique des services de renseignement et de sécurité confère à la Sûreté de l'Etat une mission générale de renseignement relative à un certain nombre d'intérêts fondamentaux de l'Etat belge.

La Sûreté de l'Etat veille, par le biais de cette mission de renseignement, à assurer la protection de ces intérêts non seulement contre toute forme d'organisation criminelle mais aussi contre toute autre forme d'activités telles qu'énumérées par l'art. 8, alinéa 1 de la loi du 30 novembre 1998.

En tant qu'activité liée au milieu du crime organisé, la traite des êtres humains est donc susceptible de rentrer dans le champ de compétences de la Sûreté de l'Etat. Les activités des organisations criminelles qui constituent une menace ne sont pas toujours de nature pénale.

Le suivi de telles menaces relève justement de la tâche spécifique du service de renseignement, qui, de cette façon, offre une protection aux institutions de l'Etat et à la société qui peut être considérée comme étant complémentaire à celle fournie par les services de police et par d'autres services administratifs.

3.1.3. Constatations faites par la Sûreté de l'État dans le cadre de la traite des êtres humains et de l'immigration illégale

Pendant la période considérée (2000 à 2002), la Sûreté de l'État s'est prioritairement intéressée aux réseaux qui se dissimulent derrière la traite des êtres humains et l'immigration illégale.

Jusqu'à ce jour, des renseignements ont été recueillis sur divers aspects fragmentaires de cette problématique. La majeure partie de ces renseignements doit encore être exploitée et approfondie par le service.

En ce qui concerne les nationalités, il peut être déduit des notes précitées que les efforts accomplis par la Sûreté de l'Etat pendant la période considérée semblent s'être principalement concentrés sur l'ancien Bloc de l'Est, l'Inde, le Pakistan, l'Afghanistan, le Sri Lanka, la Chine, l'Iran et la Turquie ainsi que les pays des Balkans.

Des Belges, naturalisés ou non, y sont également cités comme 'avocats peu scrupuleux', indépendants de mauvaise foi ou exploitants d'établissements occupant des illégaux.

Bien que des termes généraux comme ‘traite des êtres humains’ et ‘immigration illégale’ soient employés l’un pour l’autre par la Sûreté de l’Etat, il ressort à suffisance des notes en question qu’elle s’est intéressée à un ensemble de faits qui jouent un rôle dans ce contexte, qu’il s’agisse des mariages blancs, de la fabrication de faux documents, de l’occupation illégale de travailleurs, de naturalisations suspectes, etc… jusqu’aux renseignements sur des réseaux.

3.1.4. Immigration illégale et traite des êtres humains au départ de l’ex-Union soviétique

La Sûreté de l’Etat a recueilli des renseignements à propos des techniques pseudo-légales et illégales utilisées par les groupes russes du crime organisé et d’anciens citoyens soviétiques pour obtenir un titre de séjour légal en Belgique.

Une partie des informations que détient à ce sujet la Sûreté de l’Etat continue à être suivie au niveau opérationnel et analytique afin d’avoir un aperçu des réseaux qui exercent leurs activités en Belgique.

L’attention du service s’est ici particulièrement portée sur «les agences de voyages », les «négriers du logement» et les «sites internet» qui jouent un rôle dans cette problématique.

Le service réunit en outre des informations complémentaires sur le détournement de cartes professionnelles et sur la création de firmes, d’organisations internationales et d’a.s.b.l. qui pourraient intervenir dans la traite des êtres humains ou l’immigration illégale.

Le service a également apporté sa contribution dans le cadre de plusieurs affaires qui ont donné lieu à des enquêtes judiciaires. C’est ainsi que le détournement de la procédure de régularisation et de naturalisation organisé à Anvers a été suivi de près par la Sûreté de l’Etat.

Le service a, dans ce cadre également, prêté une attention particulière à la délivrance frauduleuse de visas à l’ambassade de Belgique à Sofia ainsi que de cartes d’identité spéciales.

3.1.5. Réseaux chinois

Les activités de la Sûreté de l’Etat dans le secteur des réseaux chinois font ressortir que les méthodes utilisées (mariages blancs, faux diplômes, faux liens de parenté) ainsi que les activités annexes qui y sont liées ont peu changé.

La Sûreté de l’Etat a toutefois recueilli des informations qui indiquent qu’un nombre plus important d’illégaux chinois en provenance de Fujian séjourneraient sur le territoire belge. Il se peut qu’il s’agisse d’illégaux ayant atterri chez nous lors de leur voyage vers le Royaume-Uni.

Des renseignements ont aussi été rassemblés sur une nouvelle méthode d’immigration clandestine. Cette technique consiste à se servir de fausses attestations notariales afin de certifier de faux liens de parenté entre enfants et parents.

3.1.6. Réseaux iraniens de traite des êtres humains en Belgique

La Sûreté de l'Etat a réuni des renseignements sur une bande de trafiquants d'êtres humains qui opère au départ de la Bosnie.

Pour que les candidats réfugiés de Bosnie puissent effectuer le voyage, ils se servent de faux passeports iraniens, fabriqués en Turquie.

A. Immigration illégale et traite des êtres humains en provenance des Balkans

La Sûreté de l'Etat a constaté que la traite des êtres humains en provenance des Balkans, n'est pas clairement structurée. Ce genre de traite serait aux mains de quelques individus opérant au départ de plusieurs grandes villes de Belgique.

Ces personnes bénéficieraient chaque fois du soutien d'un petit groupe de personnes de leur entourage immédiat. Le Royaume-Uni est également une destination finale de prédilection pour les illégaux originaires des Balkans.

D'après la Sûreté de l'Etat, le milieu albanais du crime organisé utilise l'immigration illégale et/ou la traite des êtres humains afin de :

- faire venir ses propres « membres » en Europe occidentale ;

- recruter parmi les illégaux des personnes pour exercer des activités criminelles ;
- faire passer en fraude des femmes en Europe occidentale pour les mettre au travail, sous la contrainte ou non, dans le milieu de la prostitution.

3.1.7. Autres réseaux

La Sûreté de l'Etat s'intéresse également aux réseaux turcs, indo-pakistanais, rwandais et kenyans, ainsi qu'à l'immigration illégale et au trafic d'êtres humains, organisé par des mouvements maffieux, extrémistes ou terroristes (GIA, PKK, LTTE).

Le réseau kurde est organisé à double sens. Une filière de la Turquie jusqu'en Europe occidentale sert à y faire parvenir des militants kurdes avec l'aide du PKK.

Ils sont ensuite recrutés et formés pour retourner dans leur pays d'origine via la deuxième filière (Belgique, Turquie). Jusqu'à la proclamation d'un cessez-le-feu unilatéral par le PKK, ces personnes étaient embrigadées par la guérilla en Turquie orientale et en Syrie.

Le réseau a aussi pour but de faire passer en fraude, en Europe occidentale, des dirigeants du PKK et les mettre ainsi en sécurité et à l'abri des poursuites des autorités turques. Dans le passé, on a même constaté le recrutement de mineurs d'âge ainsi que leur déplacement dans d'autres pays.

Le réseau pakistanais cible surtout les Sikhs. Dans la plupart des cas, leurs destinations finales sont le Royaume-Uni, le Canada ou les Etats-Unis. Une grande partie d'entre eux reste toutefois en Belgique et y travaille illégalement.

Les réseaux rwandais et kenyans sont plutôt axés sur des personnes ou des membres de leur famille qui ont participé au génocide. Ils sont ' exfiltrés' via le Kenya vers des endroits plus sûrs en Europe.

A cet effet, les Kenyans utilisent systématiquement des fausses cartes d'identité, alors que les Rwandais eux se servent d'authentiques cartes d'identité de personnes avec lesquelles il y a une forte ressemblance physique.

3.1.8. Méthode de travail

La Sûreté de l'Etat décrit comme suit ses méthodes très spécifiques d'enquête et de travail qui permettent de recueillir ces informations et de trouver des indications sur l'existence de réseaux clandestins.

Il y a tout d'abord la banque centrale de données (où sont stockées toutes les informations recueillies par le service et qui sont disponibles en fonction du 'need to know').

Ensuite, il y a l'approche résolument macro stratégique du phénomène «crime organisé - traite des êtres humains» qui permet de concentrer les faibles moyens disponibles sur les objectifs principaux. Il y a enfin le savoir-faire méthodologique spécifique de la Sûreté de l'Etat au niveau du traitement des informateurs.

Dans la pratique, le service de renseignement n'utilise pas dans ses enquêtes sur l'immigration illégale et la traite des êtres humains d'autre méthode que celle qu'il utilise dans d'autres domaines. Il essaie d'acquérir une vision aussi précise que possible de la problématique évoquée en employant des sources qui lui sont propres, c'est-à-dire, sur le plan opérationnel, en première instance, un réseau étendu d'informateurs.

3.1.9. Collaboration avec d'autres autorités

Dans le cadre de la lutte contre l'immigration illégale, la Sûreté de l'Etat collabore avec d'autres autorités telles que le Procureur fédéral, les parquets et la police fédérale.

Étant donné que le contexte de la traite des êtres humains et de l'immigration illégale est essentiellement allochtone, il n'est pas étonnant que la collaboration entre la Sûreté de l'Etat et principalement l'Office des étrangers soit bonne et ce, dans les deux sens.

C'est pourquoi la Sûreté de l'Etat dispose d'officiers de liaison à l'Office des étrangers et au Service public fédéral Affaires étrangères, qu'elle associe souvent à ses activités dans le cadre de cette problématique.

En outre, la Sûreté de l'Etat collabore à des actions concrètes contre l'immigration illégale ou la traite des êtres humains. A la suite d'une décision du gouvernement belge a été créé une Task Force «Traite des êtres humains», au sein de laquelle siègent tous les services compétents ainsi que la Sûreté de l'Etat.

La Task Force «Traite des êtres humains» s'est occupée de la création d'un Centre d'Information et d'Analyse «Traite des êtres humains»(CIAT) à laquelle la Sûreté de l'Etat a également participé.

3.1.10. La coopération internationale et la Sûreté de l'Etat

La Sûreté de l'Etat a également reçu de plusieurs services étrangers des informations (principalement à propos du vol de passeports) qu'elle a transmises aux autorités compétentes. La Sûreté de l'Etat est cependant convaincue qu'une collaboration transfrontalière est indispensable pour lutter contre l'immigration illégale et la traite des êtres humains.

La coopération de la Sûreté de l'Etat avec d'autres pays est organisée tant sur le plan européen qu'international. Cette coopération internationale entre les différents services de renseignement confrontés sensiblement aux mêmes problèmes dans la lutte contre le crime organisé s'articule tant dans un cadre multilatéral que bilatéral.

Un échange d'informations existe entre ces différents services. De plus, l'on a constitué des groupes de travail qui ciblent spécifiquement leurs activités sur la lutte contre l'immigration illégale et la traite des êtres humains.

3.1.11. Communications d'informations aux autorités judiciaires, policières et administratives

Les 147 notes précitées ont eu comme destinataires 25 autorités et services différents, les principaux étant le Magistrat national et le Procureur fédéral (105), le Ministre de la Justice (81), le Ministre de l'Intérieur (61), l'Office des étrangers (59), le Ministre et le Secrétaire-général des Affaires étrangères (59), le Premier Ministre, le Commissariat général aux réfugiés et apatrides (13), d'autres magistrats (17) et divers services de police (30).

Certaines informations ont également été transmises à des ambassadeurs et à des correspondants étrangers.

Sur base des articles 14, 19 et 20 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, des protocoles d'accords réglementant l'échange d'informations entre la Sûreté de l'Etat et les autorités judiciaires et administratives, ont été élaborés.

Ainsi, l'échange de renseignements entre la Sûreté de l'Etat et les autorités et services administratifs est réglementé par une directive du Comité ministériel du renseignement et de la sécurité du 16 février 2000.

En ce qui concerne les autorités judiciaires, la circulaire N° COL 13/99 du Collège des Procureurs généraux du 22 juin1999 prévoit spécifiquement que l'échange d'informations ou la transmission de demandes de renseignements entre la Sûreté de l'Etat et le ministère public s'effectue via les Magistrats nationaux.

Bien qu'il n'y ait pas de protocole réglementant l'échange de renseignements entre la Sûreté de l'Etat et la Police fédérale, des informations sont fréquemment transmises aux autorités policières compétentes en application des dispositions légales mentionnées plus haut.

Néanmoins, la communication d'informations classifiées aux services de police est soumise aux exigences posées par la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité. Or, en ce qui concerne les membres de la Police fédérale, l'article 24, § 4 de l'arrêté royal du 24 mars 2000 prévoit qu'en principe, il ne peut être introduit pour eux de demande d'habilitation de sécurité.

L'arrêté royal du 16 novembre 2001 modifiant celui du 24 mars 2000 permet à présent que, par dérogation au principe qui précède, une demande d'habilitation de sécurité soit être introduite pour les titulaires de certaines fonctions déterminées au sein de la Police fédérale et de la Police locale *«qui exercent une fonction nécessitant, lors d 'échanges d'informations avec les services de renseignement et de sécurité, un accès à des pièces classifiées par ceux-ci».*

La liste de ces fonctions doit être établie par le Comité ministériel du renseignement et de la sécurité. En conséquence, des informations classifiées pourraient être communiquées aux personnes titulaires de ces fonctions. Cependant, le Comité permanent R n'a pas encore eu connaissance de l'établissement de cette liste de fonctions.

Certaines notes ont toutefois fait apparaître que la nécessité de transmettre des informations prioritaires aux autorités pouvait parfois entrer en conflit avec l'obligation (légale)pour la Sûreté de l'Etat de protéger ses sources et ce en raison de l'impossibilité d'exercer un contrôle sur le grand nombre de leurs destinataires (sans habilitation de sécurité).

Pour empêcher que l'identités de ses informateurs ne soit dévoilée et pour sauvegarder le canal politique de l'information, le service ne dispose que d'un moyen : la classification. Cette dernière doit en fait être appliquée de manière inadéquate puisque les critères légaux pour les différents niveaux de classification ne sont pas applicables dans l'immense majorité des cas (et qu'en vertu de la loi on ne peut pas sur classifier).

Par ailleurs, ils compliquent sérieusement l'utilisation de l'information, par exemple par le magistrat, ce qui à son tour entraîne la nécessité de procéder à une dé-classification.

3.1.12. Spécificité de la mission de la Sûreté de l'Etat dans la lutte contre le crime organisé et la traite des êtres humains

Il convient de remarquer que le rôle de la Sûreté de l'Etat dans la lutte contre le crime organisé est différent de celui attribué aux services de police.

Les agents de la Sûreté de l'Etat n'ont aucune compétence d'officier de police judiciaire en matière de lutte contre l'immigration illégale et la traite des êtres humains. Le rôle de la Sûreté de l'Etat est en fait, en raison de sa mission de service de renseignement, de servir d'appui aux services de police.

Si le service, en cours d'enquête, acquiert connaissance de certaines affaires pouvant avoir de l'importance pour les services de police, il en informe immédiatement les autorités compétentes.

Rassembler des informations sur des faits criminels isolés ne relève pas des compétences du service. La Sûreté de l'Etat recherche les structures et les moyens d'actions de certains groupes et organisations qui peuvent constituer une menace pour la sécurité intérieure et extérieure de la Belgique.

En raison de son modus operandi, les recherches sont généralement de longue durée et n'ont pas pour résultat de fournir des preuves utilisables en justice pour des délits spécifiques, même commis par des organisations criminelles. Par conséquent, le service ne dispose pas de données quantitatives mais bien qualitatives.

Bien que la Sûreté de l'Etat n'ait pas pour tâche de rechercher des infractions, l'article 29 du Code d'instruction criminelle est pleinement applicable aux agents de la Sûreté de l'Etat dans le cadre de leurs missions.

Aux termes de cet article, « *toute autorité constituée, tout fonctionnaire ou officier public, qui, dans l'exercice de ses fonctions, acquerra la connaissance d'un crime ou d'un délit, sera tenu d'en donner avis sur-le-champ au procureur du Roi près le tribunal dans le ressort duquel ce crime ou délit aura été commis ou dans lequel l'inculpé pourrait être trouvé, et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs.* »

3.1.13. Les enquêtes menées sur l'octroi frauduleux de visas et de cartes d'identités spéciales dans des services diplomatiques belges

La Sûreté de l'Etat est bien au courant de ces deux dossiers de fraudes évoqués plus haut.

Les faits portés à la connaissance de ce service en août 1997 sont de deux ordres. Les premiers concernent la fraude proprement dite aux visas à l'ambassade de Belgique à Sofia. La Sûreté de l'Etat a pris connaissance de ces éléments, mais elle déclare n'avoir mené aucune enquête à ce sujet.

L'ambassadeur de Belgique à Sofia était suspecté par certaines personnes, qui avaient transmis certains éléments à la Sûreté de l'Etat, de travailler pour le compte des services de renseignement bulgares et de rendre des services à plusieurs personnes et firmes en rapport avec la maffia.

Un rapport interne de la Sûreté de l'Etat daté du mois de septembre 1997 indique cependant que les éléments fournis ne sont pas suffisants pour apporter la preuve que l'ambassadeur de Belgique est personnellement impliqué dans ce trafic de visas déjà connu par ailleurs de la Sûreté de l'Etat.

Le rapport indique que cet ambassadeur a par ailleurs fait l'objet d'une enquête de sécurité qui n'a révélé aucun élément défavorable.

Au cours du même mois de septembre 1997, l'administrateur général de la Sûreté de l'Etat a adressé une lettre au ministre des affaires étrangères pour le mettre au courant de faits ainsi portés à sa connaissance.

«L'exposé des faits rapportés (…) peut être divisé en deux parties :

1. La première partie concerne la prétendue fraude aux visas à l'ambassade de Belgique en Bulgarie. La Sûreté de l'Etat a pris connaissance de ces éléments mais ne mènera, cela va de soi, aucune enquête à ce sujet.

2. Une seconde partie peut être mise en rapport avec le crime organisé et concerne des entreprises et des personnes d'origine bulgare établies en Belgique. Ces personnes auraient profité de la fraude aux visas précitée, sans doute en vue de procéder au blanchiment d'argent (provenant de la maffia et/ou des services de renseignement et/ou de l'ancien parti communiste bulgare.)»

La Sûreté de l'Etat justifie au Comité permanent R l'absence d'enquête concernant la fraude aux visas de la manière suivante [161]:

«La Sûreté de l'Etat s'en est tenue jusqu'à présent à une politique de service défensif au sens strict et elle ne peut en cette qualité mener d'enquête sur les activités et contacts d'un ambassadeur à l'étranger. Il convient par ailleurs de noter qu'une enquête judiciaire était en cours concernant cette affaire et qu'il fallait à tout prix éviter une enquête parallèle de notre service.». (*lettre adressée au Comité permanent R le 5 novembre 2002 par M. Koen Dassen, Administrateur général de la Sûreté de l'Etat).*

En décembre 2000, le parquet de Bruxelles a bien reconnu l'existence d'une fraude à l'ambassade de Belgique à Sofia portant sur au moins 500 visas. Cette fraude se serait produite au cours des années 1995 à 1997. Le porte parole du parquet a ajouté que «*Sofia ne serait pas une exception* ».

Le 29 mai 2001, le Ministre des Affaires étrangères a reconnu devant la Sous-commission «Traite des êtres humains» qu'il y a bien eu un trafic de visas à l'ambassade de Belgique à Sofia, mais qu'on ne pouvait encore en identifier les responsables.

Par ailleurs en septembre 1997, la Sûreté de l'Etat avait obtenu d'autres renseignements démontrant que M.L., un fonctionnaire du Service protocole du Ministère des Affaires étrangères était impliqué dans une affaire d'octroi frauduleux de cartes d'identité spéciales.

Le dossier était lié à une affaire de traite d'êtres humains mise à l'instruction et qui concernait aussi le milieu des courses cyclistes. Comme cette affaire touchait aussi bien la criminalité organisée russe que l'espionnage, la Sûreté de l'Etat a mené son enquête en collaboration avec les autorités judiciaires.

Un rapport interne de ce service concernant cette affaire mentionne que le fonctionnaire incriminé entretenait des relations régulières avec l'ambassade de Russie, ainsi qu'avec d'autres ambassades de pays arabes et de l'Union européenne.

Le rapport souligne enfin l'absence de sensibilité à la sécurité et le manque évident de mesures de contrôle de l'accès à certains lieux et documents au sein du service Protocole, du Ministère des Affaires Etrangères.

Fin janvier 1998, une réunion s'est tenue à propos de cette affaire sur l'initiative de la Cellule «Traite des êtres humains». Cette réunion réunit le Magistrat national, un juge d'instruction, un représentant du Parquet, des enquêteurs de BSR, ainsi que des représentants de la Sûreté de l'Etat et du SGR.

Le compte-rendu de cette réunion qu'adresse le représentant de la Sûreté de l'Etat à sa hiérarchie mentionne que le parquet et le juge d'instruction sollicitent l'aide de la Sûreté de l'Etat vu la complexité du dossier et ses liens avec un ou des réseaux liant des diplomates et des hommes d'affaires russes.

[161] Traduction libre

Le rapport fait également état du *«malaise qu'éprouvent le juge d'instruction et ses enquêteurs à évoluer dans un milieu diplomatique qui ne leur est pas familier. (…) Une tendance à vouloir laver le linge sale en famille de la part du Protocole donne aux enquêteurs l'impression de gêner et l'abord de ces hauts fonctionnaires et personnes jouissant de certaines immunités ne facilite pas les devoirs d'enquête».*

Ce même rapport mentionne pourtant qu'il serait intéressant pour la Sûreté de l'Etat de connaître les contacts du fonctionnaire incriminé aussi bien au niveau professionnel qu'au niveau privé. La suite du dossier, dont le Comité permanent R a pris connaissance, démontre pourtant que la Sûreté de l'Etat n'a entrepris aucune démarche en ce sens.

La Sûreté de l'Etat avait déjà eu auparavant connaissance d'autres affaires de fraude et en avait averti les autorités compétentes.

Questionnée plus avant sur ces affaires, la Sûreté de l'Etat a fourni au Comité permanent R quelques informations complémentaires classifiées «SECRET» d'où il ressort qu'il s'agissait d'une part, d'interventions auprès de l'Office des étrangers en vue de l'octroi de permis de séjours et d'autre part, de faux visas accordés à des hommes d'affaires étrangers, surtout actifs dans le commerce des diamants.

A la question de savoir si des enquêtes de sécurité concernant le personnel diplomatique avaient relevé des implications dans ce type de trafic au niveau de la délivrance des visas, la Sûreté de l'Etat a répondu que *«les enquêtes (…) menées sur le personnel diplomatique n'ont jusqu'à présent apporté aucun élément indiquant leur implication dans un trafic de visas».*

Au cours de l'année 2001, la Sûreté de l'Etat reçut pourtant d'un informateur occasionnel une note posant la question de savoir si les pratiques frauduleuses dénoncées étaient uniquement imputables à un fonctionnaire subalterne du ministère des Affaires étrangères ou s'il fallait aussi penser à d'éventuelles complicités de supérieurs hiérarchiques et/ou à leur incompétence au niveau des contrôles.

La fiabilité de cet informateur ayant été mise en doute, la Sûreté de l'Etat n'a réservé aucune suite à ce rapport. Aucune vérification complémentaire n'a été effectuée pour vérifier l'hypothèse émise par cette source.

A défaut donc d'avoir enquêté sur les fraudes elles-mêmes et sur les liens éventuels que leurs auteurs présumés entretenaient avec des pays étrangers ou des organisations criminelles, la Sûreté de l'Etat a plutôt enquêté sur les personnes qui ont bénéficié de ces fraudes. A cet égard, la collaboration du service avec les autorités judiciaires semble avoir été effective.

Dans les rapports concernant les faux visas accordés à l'ambassade belge de Sofia, la Sûreté de l'Etat s'attache principalement aux activités commerciales menées en Belgique par l'un des bénéficiaires bulgares de ces faux visas. Le Comité n'a pas connaissance de la suite donnée par le pouvoir judiciaire à ces informations, ni des résultats de l'enquête.

En ce qui concerne les fausses cartes d'identité spéciales octroyées par un fonctionnaire du ministère des Affaires étrangères, la Sûreté de l'Etat a communiqué au Magistrat national l'identité d'une quarantaine de ressortissants russes ayant bénéficié de ces fausses cartes.

Il s'agissait notamment d'hommes d'affaires, parfois de grande envergure et impliqués dans d'importantes tractations industrielles avec la Belgique, de sportifs et de diplomates dont certains étaient connus pour leurs activités d'espionnage ou de lobbying.

En juillet 2001, en réponse à la demande d'information du ministre, l'Administrateur général de la Sûreté de l'Etat lui fait savoir que son service mène une enquête sur l'implication de la criminalité organisée et des services de renseignement russes dans l'affaire des fausses cartes d'identité délivrées par M. L.[162] :

«Aucun lien structurel n'a pu être établi. Plusieurs acquéreurs de ces cartes d'identité spéciales ont toutefois été identifiés par la Sûreté de l'Etat comme proches de la criminalité organisée».

3.2. Le SGRS

Le 15 janvier 2004, en réponse aux questions posées par le Service d'enquêtes du Comité permanent R le SGRS a fait savoir qu'il avait connaissance de faits récents en relation avec une affaire de faux passeports délivrés dans un pays d'Afrique et l'implication de ressortissants belges dans ce trafic.

Le SGRS en a averti la Sûreté de l'Etat.

Le SGRS a également eu connaissance d'une affaire mettant en cause un consul général de Belgique dans un pays d'Afrique du Nord.

4. L'ANALYSE DU CENTRE POUR L'ÉGALITÉ DES CHANCES ET LA LUTTE CONTRE LE RACISME (CECLR)

Dans son rapport annuel de mai 2001, le Centre pour l'égalité des chances et la lutte contre le racisme (CECLR) consacre une section à l'analyse des pratiques de trafics de visas et de documents de séjour dans les anciens pays du bloc de l'Est. Le Comité permanent R ne peut s'empêcher de reproduire ici ce texte in extenso.

«L'analyse des pratiques de trafic de visas et de documents de séjour nous a menés aussi en partie, même limitée, aux maffias russes (et leurs satellites), représentants de l'ancienne URSS.

Dans la littérature, il est signalé de manière générale que les anciens services secrets de l'ex-URSS ont, au moment où ils ont compris que les régimes communistes viendraient à imploser en Europe de l'Est, établi les contacts nécessaires avec des personnes et institutions occidentales pour, avant tout, organiser la fuite des capitaux vers l'Occident.

Les meilleurs agents de liaison avec l'Ouest étaient à l'époque les sportifs (et leurs épouses) et le personnel accompagnant. Il est frappant en particulier de voir, et tant en Bulgarie qu'en Russie, combien d'anciens lutteurs, cyclistes et ex-policiers ont pu, après la chute du régime, démarrer de brillantes carrières à la tête d'entreprises et banques privées. Pour réussir dans le trafic de devises, l'aide de personnes issues ou gravitant autour des ambassades occidentales était cependant nécessaire.

Il fallait ensuite s'infiltrer dans les administrations officielles des pays occidentaux.

[162] Traduction libre

L'obtention de toute forme de documents de séjour officiels, par le biais desquels la libre circulation à l'intérieur des pays occidentaux, au sein de l'espace Schengen se réalise, était la première priorité de ces agents du KGB à la recherche de places pour leurs opérations de blanchiment d'argent.

Dans le sillage du trafic de documents, d'autres formes de trafic ont suivi : de la traite des êtres humains en vue de toute sorte d'autres trafics – et c'est la majorité – à la simple organisation de l'immigration illégale.

Ce sont principalement les administrations qui ne sont pas soumises à un contrôle extérieur, comme c'est encore une fois le cas des services rattachés à l'administration des Affaires Etrangères - et ceci n'est pas un phénomène exclusif à la Belgique, qui sont particulièrement vulnérables à ce type de pratiques.

Tout d'abord parce qu'elles peuvent délivrer des documents particulièrement intéressants à des personnes aux intentions mafieuses, et ensuite parce que cela peut durer des années avant que quelqu'un ne découvre les irrégularités ou la négligence.

Les négligences dans le cadre de la délivrance des visas Schengen à ce type de personnes ou organisation mafieuses au sein de presque toutes les ambassades occidentales (et services du protocols ?) sont devenues de notoriété publique.
Ces pratiques semblent tellement éloignées d'une gestion normale des affaires publiques (qui tombent normalement sous le contrôle du parlement) qu'elles ne font jamais l'objet d'un point central dans les débats parlementaires ou médiatiques».

Et le CECLR conclut à ce propos :

«Il convient aujourd'hui de faire certaines propositions afin de trouver des solutions à cette problématique », notamment *« prévoir une sensibilisation par le biais du Ministère des Affaires étrangères des différentes ambassades sur la problématique tout en renforçant le contrôle d'octroi de visas touristiques. Il convient absolument de stipuler la raison réelle pour laquelle la personne demande l'octroi d'un visa. Si le visa est demandé par un club pour un test ? il convient de limiter la durée du séjour à la durée du test»*.

En juin 2001, le Ministère des Affaires étrangères a annoncé un renforcement des contrôles des procédures d'octroi des visas dans les ambassades.

Dans son rapport d'activités pour l'année 2002, le CECLR revient sur cette problématique pour souligner la nécessité d'une approche intégrée de la lutte contre la traite des êtres humains, à défaut de quoi celle-ci menace alors de devenir une lutte symptomatique focalisée sur la chasse aux illégaux.

Le CECLR constate que de tels trafics sont souvent accompagnés d'affaires de faux papiers et de corruption mafieuse. « *Et qui dit mafia sait ce que cela signifie : intimidation, infiltration dans les institutions et corruption* » ajoute le CECLR.

La Commission d'enquête parlementaire du Sénat chargée de l'enquête sur la criminalité organisée n'avait-elle d'ailleurs pas, elle aussi, conclu que la fraude de documents était le fil rouge de la criminalité organisée[163] ? Et le CECLR de citer aussi le rapport de la justice sur la criminalité organisée qui établit que la mafia russe tente de s'infiltrer dans l'appareil d'Etat[164].

---

163 Doc. Parl. Sénat, 1-326/9, p. 531

164 Justice, rapport annuel, "La criminalité organisée en Belgique en 2000", p. 65

Le CECLR préconise donc la mise en place d'un service qui puisse combattre la corruption de manière structurée et il souligne le rôle que la Sûreté de l'Etat est susceptible de jouer dans cette matière.

5. LE POINT DE VUE DE PARLEMENTAIRES BELGES ET RUSSES

Le 9 juillet 2002, la commission de l'Intérieur et des Affaires administratives du Sénat de Belgique a rendu public un rapport rédigé en commun avec le Comité pour la sécurité de la Douma de la Fédération de Russie [165].

Ce document intitulé *«Russie - Belgique : deux visions de la migration »* présente une série de constatations et d'analyses effectuées ensemble par les parlementaires russes et belges à propos de la migration, de ses causes et de ses effets.

Tout en plaidant pour une politique active de lutte contre l'inégalité sociale et la pauvreté au niveau international afin de combattre les causes structurelles de l'immigration, les parlementaires russes et belges en appellent également à renforcer la lutte concertée contre l'immigration illégale, afin de mieux combattre la menace du terrorisme international, de la criminalité organisée transnationale et pour défendre les intérêts étatiques de la Belgique et de la Russie.

Et le rapport de conclure notamment que *« les meilleurs résultats en vue d'atténuer l'acuité de ce problème sont atteints s'il existe un organe dirigeant qui organise la lutte contre ce phénomène, une interaction concertée de tous les services policiers et spéciaux (de la police, des services de renseignements, etc.) »*

6. CONCLUSIONS

6.1. Sur la manière dont la Sûreté de l'État traite la matière de la traite des êtres humains en général

Après la décision prise par le gouvernement en août 2001 d'inscrire la problématique de la traite des êtres humains parmi ses priorités, rien ou quasiment rien n'a en fait changé pour les services chargés de suivre cette matière dans leur manière de recueillir et d'analyser les informations.

Ce sujet faisait en effet déjà l'objet d'un suivi, mais en tant que « phénomène marginal ». Dès la mi-2001, les autorités furent régulièrement tenues au courant et le nombre des destinataires des notes a été élargi 'sur le terrain'. Quant à savoir si l'information transmise est d'une quelconque 'utilité', c'est là le sujet éventuel d'autres enquêtes.

165 Sénat de Belgique, session 2001-2002, 9 juillet 2002, 2 - 920 / 1

Des informations furent échangées avec des services étrangers de renseignement et l'on a pu constater clairement l'existence d'une coopération bilatérale intérieure avec d'autres services officiels comme principalement l'Office des étrangers, le Commissariat général aux réfugiés et apatrides, la Cellule «Traite des êtres humains» de la Police fédérale, les Affaires économiques et l'Inspection sociale.

De plus, il y a également des initiatives récentes telles que le fait d'avoir associé la Sûreté de l'Etat à la création du CIAT ainsi qu'à la réunion préparatoire et à la réunion proprement dite du groupe de travail européen CIREFI (Centre d'Information, de Réflexion et d'Echange d'informations pour le Franchissement des frontières et l'Immigration).

Etant donné que les activités de la Sûreté de l'Etat sont en première instance axées sur les faits et gestes politiques dans les colonies qu'elle suit et que la traite des êtres humains/l'immigration illégale n'y constituent qu'un phénomène marginal, elle peut et a même tendance à établir des liens sous un autre angle que les autorités et les services qui ne s'occupent que de l'aspect pénal des choses.

Grâce à ses contacts avec divers services et à l'échange d'informations avec des informateurs étrangers, la Sûreté de l'Etat peut avoir un aperçu des réseaux internationaux et aussi établir des liens entre revendications politiques et activités criminelles de certaines organisations activistes.

La mesure dans laquelle le service est au courant de ce qui est à suivre au sein d'une communauté nationale donnée dépend souvent de circonstances dues au hasard, mais certaines notes indiquent que la Sûreté de l'Etat était bien implantée dans certaines colonies et que « l'information politique traditionnelle » pouvait être recueillie sans trop de difficultés.

Ce genre de prestations requiert évidemment du temps et du savoir-faire pour le recrutement d'informateurs dont les activités de la Sûreté de l'Etat dépendent dans une large mesure.

Certaines notes ont toutefois fait apparaître que la nécessité de transmettre des informations prioritaires aux autorités pouvait parfois entrer en conflit avec l'obligation (légale) pour la Sûreté de l'Etat de protéger ses sources et ce, en raison de l'impossibilité d'exercer un contrôle sur le grand nombre de destinataires qui ne sont pas toujours titulaires nécessairement d'une habilitation.

6.2. Concernant l'octroi frauduleux de visas et de cartes d'identités spéciales dans des services diplomatiques belges

La Sûreté de l'Etat est bien au courant de ces deux dossiers de fraudes évoqués ci-avant. Ce service avait déjà eu auparavant connaissance d'autres affaires de fraude et en avait averti les autorités compétentes. Il s'agissait d'interventions auprès de l'Office des étrangers en vue de l'octroi de permis de séjours et de faux visas accordés à des hommes d'affaires étrangers, surtout actifs dans le commerce des diamants.

Le Comité permanent R a cependant constaté que la Sûreté de l'Etat n'avait enquêté, ni sur les fraudes elles-mêmes, ni sur les liens éventuels que leurs auteurs présumés étaient suspectés d'entretenir avec des pays étrangers ou des organisations criminelles.

Un rapport interne indiquait pourtant qu'il serait intéressant pour la Sûreté de l'Etat de connaître les contacts du fonctionnaire incriminé, aussi bien au niveau professionnel qu'au niveau privé. La suite du dossier dont le Comité permanent R a pris connaissance démontre que la Sûreté de l'Etat n'a toutefois entrepris aucune démarche en ce sens.

De même, au cours de l'année 2001, la Sûreté de l'Etat n'a donné aucune suite à des informations reçues d'un informateur occasionnel évoquant la complicité possible (ou tout au moins l'incompétence) de certains fonctionnaires de niveau supérieur dans les fraudes aux documents évoquées.

La Sûreté de l'Etat justifie au Comité permanent R l'absence d'enquête concernant la fraude aux visas à Sofia de la manière suivante[166] :

«La Sûreté de l'Etat s'en est tenue jusqu'à présent à une politique de service défensif au sens strict et elle ne peut en cette qualité mener d'enquête sur les activités et contacts d'un ambassadeur à l'étranger. Il convient par ailleurs de noter qu'une enquête judiciaire était en cours concernant cette affaire et qu'il fallait à tout prix éviter une enquête parallèle de notre service». (Lettre adressée au Comité permanent R le 5 novembre 2002 par M. Koen Dassen, Administrateur général de la Sûreté de l'Etat).

A la question de savoir si des enquêtes de sécurité concernant le personnel diplomatique avaient relevé des implications dans ce type de trafic au niveau de la délivrance des visas, la Sûreté de l'Etat a répondu que *«les enquêtes (…) menées sur le personnel diplomatique n'ont jusqu'à présent apporté aucun élément indiquant leur implication dans un trafic de visas»*[167].

Le Comité permanent R ne peut s'empêcher de partager l'impression décrite par un inspecteur de la Sûreté de l'Etat dans l'un des rapports relatifs à ces enquêtes, à savoir : *« une tendance à vouloir laver le linge sale en famille de la part du Protocole »* ce qui *« donne aux enquêteurs l'impression de gêner ces hauts fonctionnaires et personnes jouissant de certaines immunités* » et qui ne facilite pas les devoirs d'enquête. *C'est ainsi que, plutôt que d'enquêter sur les auteurs des fraudes, la Sûreté de l'Etat a plutôt enquêté sur les personnes qui en ont bénéficié.*

A cet égard, la collaboration du service avec les autorités judiciaires semble avoir été effective. La Sûreté de l'Etat a communiqué au Magistrat national l'identité d'une quarantaine de ressortissants russes ayant bénéficié de ces fausses cartes belges.

Il s'agissait notamment d'hommes d'affaires, parfois de grande envergure et impliqués dans d'importantes tractations industrielles avec la Belgique, de sportifs et de diplomates dont certains étaient connus pour leurs activités d'espionnage ou de lobbying.

Néanmoins, la Sûreté de l'Etat reconnaît qu'elle n'a pu établir :

- aucun lien direct entre l'affaire des faux visas de l'ambassade de Belgique en Bulgarie et celle des fausses cartes d'identité spéciales du service protocole;
- aucun lien structurel entre ces affaires et la criminalité organisée,
- aucun rapport entre ces deux affaires et un éventuel trafic d'êtres humains, bien qu'un lien existe entre la criminalité organisée russe et le milieu cycliste professionnel parfois cité comme filière pour ce type de trafic.

[166] Traduction libre
[167] idem

Le Comité permanent R regrette cependant que la Sûreté de l'Etat n'ait pas été en état de produire une synthèse et une analyse globale des pratiques dénoncées par le CECLR dans son rapport de mai 2001, à savoir *«l'infiltration des milieux officiels par des milieux criminels organisés afin d'obtenir des faux visas et documents permettant le séjour en Belgique.»*

6.3. Concernant le SGRS

Le SGRS n'a pas compétence pour enquêter sur des affaires de fraudes aux documents ni sur la traite des êtres humains. Ce service a communiqué certaines informations à la Sûreté de l'Etat à propos d'une affaire de fraude aux documents dont il a eu connaissance.

7. RECOMMANDATIONS

La lecture du rapport d'activités 2001 du *Binnenlandse Veiligheidsdienst* (BVD, le service de renseignement civil néerlandais) nous apprend que ce service est investi de missions de sécurité en rapport avec les deux problématiques évoquées ci-dessus, à savoir la production et la distribution de documents officiels permettant l'accès au territoire d'une part, l'intégrité des agents de la fonction publique d'autre part.

DISTRIBUTION ET DÉLIVRANCE DE DOCUMENTS DE VOYAGE

Depuis 1999, le BVD est associé au projet « nouvelle génération » de documents de voyage. Le BVD fait office, pendant toute la durée du projet, de conseiller en matière de protection de la production, de la distribution et de la délivrance du nouveau document de voyage ainsi qu'en matière de protection des réseaux d'information et de communication entre le producteur des documents et les instances qui en demandent.

Le BVD continuera à être associé à la protection du nouveau document de voyage puisque des fonctions de confiance sont à prévoir chez le producteur des documents et que le BVD a donc pour mission d'effectuer des enquêtes de sécurité à propos des candidats à ces fonctions.

INTÉGRITÉ DE L'ADMINISTRATION PUBLIQUE

L'intégrité de l'administration a une importance effective pour la qualité de l'ordre juridique démocratique. Des pouvoirs publics qui ne sont pas intègres perdent en effet la confiance du citoyen et par là leur légitimité. Sans confiance ni légitimité, une démocratie ne peut pas fonctionner.

Dans le présent paragraphe, sont explicités les deux points sur lesquels le BVD apporte sa contribution en matière d'intégrité. Le premier est le soutien au niveau des enquêtes de vulnérabilité que des organismes publics peuvent mener eux-mêmes. En outre, le BVD est habilité a recevoir des informations concernant de possibles atteintes à l'intégrité de l'autorité ou de l'administration.

A. Encadrement des enquêtes de vulnérabilité

Depuis 1966, le BVD suscite et encadre des enquêtes de vulnérabilité au sein des instances de l'autorité publique. Ces enquêtes visent à donner un aperçu des processus et des fonctions qui au sein d'organisations, sont vulnérables du point de vue de l'intégrité.

Les enquêtes sont en premier lieu effectuées par les organisations elles-mêmes. Le cas échéant, le BVD peut (sur demande) encadrer l'enquête, mais à distance.

En 2002, partant des expériences acquises dans la pratique, le BVD a revu son manuel *«Een beetje integer kan niet» («On ne peut être intègre qu'à moitié»)*. Lors de cette révision, l'accent a surtout été mis sur le développement de l'effort personnel sur la convivialité de l'utilisation et l'actualité.

Au début de 2001, le service a été invité, dans le cadre d'un projet subsidié par l'Union européenne, à communiquer son savoir-faire dans le domaine de l'exécution de ce genre d'enquête à un certain nombre de fonctionnaires d'Estonie. Le BVD a ainsi apporté son aide au service de la Sûreté d'Estonie.

B. Le point de contact pour les atteintes à l'intégrité

Le point de contact «atteintes à l'intégrité» est un service au sein du BVD auquel tout un chacun peut signaler des atteintes présumées à l'intégrité de l'autorité et de l'administration.

Ces informations reçues sont préalablement examinées sous trois aspects avant que le BVD n'entame lui-même une enquête éventuelle. Il faut en tout premier lieu qu'il y ait une atteinte à l'intégrité dans l'administration publique.

En deuxième lieu, il faut que cette atteinte entre dans le cadre légal des missions du BVD et soit donc une atteinte à l'ordre juridique démocratique, à la Sûreté de l'Etat ou à d'autres intérêts importants de l'Etat.

Enfin, il ne faut pas qu'une autre instance soit compétente pour traiter cette information ou la traite déjà. Lorsqu'il est satisfait à toutes ces conditions, et qu'il est possible et pas improbable qu'il y ait en effet une violation de l'intégrité, le BVD procède à une enquête conformément à la loi sur les services de renseignement et de sécurité, le BVD veille à protéger en toutes circonstances l'identité de la personne qui lui a communiqué des informations.

Le Comité permanent R recommande par conséquent qu'à l'instar du service néerlandais BVD, la Sûreté de l'État reçoive la mission de :

- ***s'intéresser aussi bien aux auteurs qu'aux bénéficiaires des trafics de visas, de passeports et de tous autres documents d'identité belges ;***

- ***s'intéresser aux vulnérabilités de certains services essentiels de l'État et notamment aux influences possibles que des réseaux criminels ou des services de renseignement étrangers sont susceptibles d'exercer à l'égard des membres du personnel diplomatique ;***

- ***d'enquêter à cet égard dans les ambassades et autres postes diplomatiques belges établis dans des pays sensibles au départ desquels un trafic d'êtres humains est susceptible d'être organisé ;***

- ***de soumettre l'ensemble du personnel diplomatique et administratif de ces ambassades à des enquêtes de sécurité approfondies ;***

- ***de sensibiliser le personnel du ministère des Affaires étrangères sur les mesures de sécurité à prendre dans leurs locaux et sur les manœuvres d'approches et de manipulations que ces fonctionnaires pourraient subir de la part de personnes mêlées à des trafics de visas et de documents de séjour.***

CHAPITRE 4: RAPPORT DE L'ENQUÊTE SUR LE COMPORTEMENT D'UN AGENT ADMINISTRATIF DE LA SÛRETÉ DE L'ETAT

1. INTRODUCTION

A l'occasion d'une audition effectuée en avril 2001 dans le cadre d'une autre enquête que celle qui fait l'objet du présent rapport, le Service d'enquêtes R a été mis au courant d'un fait susceptible de constituer aussi bien un abus de fonction qu'une violation du devoir de secret professionnel dans le chef d'un agent de la Sûreté de l'Etat.

L'agent en question (Monsieur. X) aurait tenté d'obtenir un avantage financier auprès d'un inspecteur de fraudes aux assurances en lui dénonçant une escroquerie d'une part, en invoquant sa qualité d'agent de la Sûreté de l'Etat d'autre part et en lui déclarant que ce service menait une enquête sur l'un des supposés protagonistes de l'escroquerie.

2. PROCEDURE

Le 7 juin 2001, le Service d'enquêtes R entendit l'inspecteur de fraudes qui aurait reçu la dénonciation de Monsieur X. Cette audition fit apparaître l'éventualité d'une dénonciation calomnieuse de la part de Monsieur X apparemment guidé par des ressentiments personnels.

Le 16 juillet 2001, le Service d'enquêtes R adressa au Comité permanent R une note d'information sur ces faits.

Suite à cette communication, le Comité permanent R décida le 25 juillet 2001 d'ouvrir une enquête d'initiative sur le comportement d'un agent administratif de la Sûreté de l'Etat.

Une apostille fut adressée au chef du Service d'enquêtes le 22 août 2001.

Le président du Sénat et le ministre de la Justice furent avertis de l'ouverture de l'enquête le 27 août 2001.

Au cours des mois d'août, de septembre et d'octobre 2001, le Service d'enquête R a procédé à l'audition des personnes citées dans l'affaire, parmi lesquelles l'agent incriminé de la Sûreté de l'Etat. Le dossier de l'enquête de sécurité de l'intéressé a été examiné.

Au cours du mois de décembre 2001, le Service d'enquêtes R a pu consulter les procès-verbaux rédigés par les services de police à propos de cette affaire.

Le Service d'enquête a remis son rapport au Comité permanent R le 20 décembre 2001.

Le présent rapport a été approuvé le 11 décembre 2003.

Le rapport a été envoyé pour avis au Ministre de la Justice le 6 janvier 2004. Par sa lettre du 21 janvier 2004 le Ministre nous a fait savoir ce qui suit : « *Je n'ai pas d'observations particulières à formuler à ce sujet et donne instruction à la Sûreté de l'Etat pour que les devoirs d'information, de discrétion et de prudence qui incombent aux membres de ce personnel, soient davantage explicités lors de leur entrée en fonction ».*

3. CONSTATATIONS

3.1. La dénonciation de Monsieur X., agent de la Sûreté de l'État

Monsieur Y., inspecteur de fraudes auprès d'une compagnie d'assurance, a effectivement reçu au mois de mars de l'année 2000 une dénonciation de Monsieur X., agent de la Sûreté de l'Etat. Monsieur X. admet qu'il a fait état à Monsieur Y. de sa qualité d'agent de la Sûreté de l'Etat.

La dénonciation se rapportait à un accident de la circulation qui aurait été simulé en 1997 par des particuliers en vue d'obtenir le remboursement des véhicules déclassés auprès des compagnies d'assurance.

Selon l'inspecteur de fraudes, Monsieur X. aurait en outre déclaré que l'une des personnes qu'il citait dans l'affaire faisait l'objet d'une enquête de la part de la Sûreté de l'Etat. Cette dernière allégation a été vérifiée par le Service d'enquêtes R : la personne citée n'est absolument pas connue dans les fichiers de la Sûreté de l'Etat. Il n'apparaît donc pas que Monsieur X. aurait violé un secret professionnel, mais plutôt qu'il aurait menti.

Selon l'inspecteur de fraudes, Monsieur X. aurait sollicité un avantage financier en contrepartie de ses révélations. Monsieur X. déclare à cet égard que s'il a effectivement fait allusion à une certaine gratification que pourraient recevoir les personnes qui permettent de récupérer l'argent de l'assurance indûment perçu, l'inspecteur de fraude s'est toutefois mépris sur ses intentions, qu'il avait mal compris ses propos, qu'il ne s'agissait que d'une plaisanterie.

L'inspecteur de fraudes déclara également qu'à l'occasion d'un contact téléphonique ultérieur, Monsieur X. s'était informé des suites de sa dénonciation. N'ayant reçu qu'une réponse vague de Monsieur Y., Monsieur X. lui aurait demandé s'il avait peur car il risquait de mettre les pieds dans une « grosse affaire ». Monsieur X. affirme pour sa part qu'il n'a plus jamais repris contact avec Monsieur Y. après lui avoir dénoncé les faits.

Bien que Monsieur X. ne lui ait apporté aucune preuve formelle établissant l'existence d'une escroquerie, Monsieur Y. l'inspecteur de fraudes porta toutefois plainte auprès de la gendarmerie locale en juin 2000. Il souhaitait en effet faire toute la lumière sur cette affaire compte tenu de certains éléments du dossier et de la qualité professionnelle qu'invoquait la personne lui ayant rapporté les faits. L'enquête menée par la gendarmerie au cours des mois de juin et d'août 2000, au cours de laquelle Monsieur X. fut entendu, n'apporta aucun élément permettant de conclure à la réalité de l'escroquerie dénoncée par ce dernier.

Dans une déclaration faite au Service d'enquêtes R, Monsieur X. déclare que lors de son audition, « *le gendarme m'a clairement fait comprendre que je n'avais pas intérêt à persister dans mes affirmations si je ne voulais pas d'ennui dans ma carrière ; j'ai donc décidé de laisser tomber alors que dans le fond, j'étais certain de mes dires* ».

Selon certaines personnes auditionnées au cours de cette enquête de gendarmerie, la dénonciation de Monsieur X. était motivée par des ressentiments personnels à leur égard. Néanmoins, aucune poursuite judiciaire ne fut intentée à l'égard de Monsieur X. pour dénonciation calomnieuse.

Ainsi Madame Z., l'une des personnes auditionnées par la police, signala qu'elle avait été autrefois la compagne de Monsieur X. et que ce dernier utilisait « *les facilités de son travail à la Sûreté de l'Etat* » pour la suivre à la trace et tenter de lui nuire depuis sa séparation.

Monsieur X admet qu'il a eu connaissance des faits supposés d'escroquerie par Madame Z. alors qu'il la fréquentait mais il nie avoir profité de sa fonction à la Sûreté de l'Etat pour importuner qui que ce soit dans cette affaire.

3.2. Situation de Monsieur X. à la Sûreté de l'État

Le Service d'enquêtes R a vérifié que Monsieur X était effectivement un agent administratif de la Sûreté de l'Etat ; celui-ci était relativement nouveau dans la maison.

Le dossier établi en vue de l'octroi à l'intéressé d'une habilitation de sécurité du niveau « très secret » a été examiné.

Une première enquête effectuée en 1995 n'a rien révélé de défavorable à son sujet.

A une date indéterminée mais postérieure à l'été 1997, Monsieur X s'est rendu dans un pays qui appartenait autrefois au bloc de l'Est pour un motif d'ordre privé. Se référant à une note de service du 23 juin 1997 levant toute restriction aux voyages privés à l'étranger pour le personnel de la Sûreté de l'Etat, l'intéressé n'a pas signalé ce déplacement à l'étranger à sa hiérarchie. La note de service précitée prescrit cependant que « *la discrétion et la prudence s'imposent toujours, en particulier en ce qui concerne certains pays* ». En cas de doute, les agents sont priés de consulter le Commissaire en chef.

Au cours du mois de juin de l'année 2000, lorsque l'intéressé a signé une demande de renouvellement de son habilitation de sécurité, celui-ci a omis d'y signaler son mariage contracté à l'étranger avec une ressortissante étrangère. L'intéressé a d'ailleurs rayé sur le formulaire ad hoc la mention pré imprimée selon laquelle les informations fournies par lui étaient complètes. Plus tard, en septembre de la même année, Monsieur X. a signé une nouvelle demande d'habilitation de sécurité dans laquelle il a, alors, signalé le mariage qu'il avait contracté à l'étranger. Monsieur X. a justifié sa première omission par le fait qu'à ce moment, son mariage n'avait pas encore été « légitimé » en Belgique.

Le Comité permanent R note à cet égard que deux notes de service de la Sûreté de l'Etat, (l'une datée du 28 mai 1953, l'autre du 8 juillet 1971, il est vrai), prescrivent aux membres du personnel, tant administratif que des services extérieurs, de signaler tout projet de mariage. « *Cette communication mentionnera spécialement l'identité, la nationalité ainsi que la résidence de la fiancée* ».

Il n'apparaît pas que cette instruction ait été abrogée depuis lors. Il n'apparaît pas non plus que cette instruction ait été rappelée au personnel dans une note plus récente.

L'enquête de sécurité consécutive à la demande de renouvellement de l'habilitation de sécurité de Monsieur X. ne révéla rien de défavorable, ni sur lui-même, ni sur son épouse. Le rapport d'enquête signale d'ailleurs que Monsieur X. est inconnu auprès des services de police communale et judiciaire. L'enquête de sécurité réalisée à son sujet n'a donc pas fait apparaître qu'il avait été entendu quelques temps auparavant par la gendarmerie à propos de sa dénonciation d'une prétendue escroquerie à l'assurance.

L'habilitation de sécurité de Monsieur X. fut donc renouvelée au niveau « très secret », mais celle-ci fut limitée à un an, au motif que l'intéressé avait omis de signaler son mariage à l'étranger.

Peu après son audition par le Service d'enquêtes R, Monsieur X. signala à son officier de sécurité qu'il ne donnerait plus son accord pour qu'une nouvelle enquête de sécurité soit menée à son sujet.

Cet accord étant indispensable[168], il ne put donc être procédé à une nouvelle enquête de ce type au cours de l'année 2002.

L'intéressé a donc fait l'objet d'une mesure de mutation interne au ministère de la Justice ; celui-ci ne fait plus partie du personnel de la Sûreté de l'Etat depuis l'année 2002.

4. CONCLUSIONS

Au-delà des faits ponctuels et des allégations divergentes, voire contradictoires, des protagonistes de cette affaire, celle-ci interpelle le Comité permanent R sur plusieurs questions de principe :

- Les nouveaux arrivants à la Sûreté de l'Etat sont-ils suffisamment informés de leurs devoirs de discrétion et des obligations particulières qui en découlent, comme par exemple celle de ne pas faire état inutilement de leur appartenance à ce service dans leurs rapports avec des tiers, celle de signaler un projet de mariage ?

- En ce qui concerne les voyages privés à l'étranger, la note de service du 23 juin 1997 relative aux voyages privés à l'étranger est-elle suffisamment claire pour le personnel lorsqu'elle indique que la discrétion et la prudence s'imposent en ce qui concerne « certains pays » non autrement identifiés ? Ne conviendrait-il pas d'être plus précis à ce sujet ?

- Les agents de la Sûreté de l'Etat disposent-ils d'ailleurs d'un manuel contenant les instructions permanentes de sécurité et autres en vigueur dans le service ? [169]

---

168 Article 16 § 1er de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité.

169 Selon une enquête du Comité permanent R, menée en 1995, les directives internes de la Sûreté de l'Etat se présentaient alors comme une suite non coordonnée de circulaires, de notes et d'ordres de service émis (ou abrogés) à tout moment. La situation ne semble pas avoir changé depuis lors. Les ordres permanents du SGRS par contre étaient rassemblés dans un corpus d'instructions codifiées, coordonnées et régulièrement mises à jour. Ce corpus, précédé d'une table des matières, était l'instrument auquel chaque membre du service pouvait se référer en permanence. Le Comité permanent R avait donc recommandé que la Sûreté de l'Etat établisse, elle aussi, un code de règles permanentes, claires et classées par thèmes auquel le personnel puisse se référer.

– La décision de limiter à un an [170] la durée de validité de l'habilitation de sécurité de Monsieur X. ne constitue-t-elle pas, en l'espèce, une mesure disciplinaire déguisée à son encontre, plutôt qu'une réelle mesure de sécurité ? Le non-respect d'une instruction interne de la part de l'intéressé ne justifiait-il pas une sanction disciplinaire ?

– Monsieur X. ayant refusé de donner son accord à une nouvelle enquête de sécurité sur sa personne, celui-ci fut muté dans un autre service du ministère de la Justice puisqu'il ne satisfaisait plus à l'obligation d'être titulaire d'une habilitation de sécurité pour occuper une fonction à la Sûreté de l'Etat. Que serait-il advenu de Monsieur X. si ce dernier avait été membre d'un des services extérieurs de la Sûreté de l'Etat ?

  Le statut de ces agents prévoit en effet la nécessité d'être titulaire d'une habilitation de sécurité pour être nommé dans ces services (article 16, 7° de l'arrêté royal du 22 août 1998 portant statut des membres des services extérieurs de la Sûreté de l'Etat). Or le principe de la « barrière » qui est également prévu par ce même statut (article 3 de l'arrêté royal précité) empêche en effet toute mobilité de ces agents vers d'autres services de l'administration fédérale.

5. RECOMMANDATIONS

Le Comité permanent R recommande :

– comme il l'avait déjà fait en 1995, d'élaborer un corpus coordonné et mis à jour des instructions permanentes en vigueur au sein de la Sûreté de l'Etat, notamment en ce qui concerne les obligations particulières imposées au personnel en matière de sécurité ;

– de fournir ce corpus d'instructions permanentes à chaque membre du personnel ;

– de préciser le contenu de l'ordre de service du 23 juin 1997 en ce qui concerne les pays à l'égard desquels la discrétion et la prudence s'imposent au personnel lors de voyages privés ;

d'assouplir le principe de la barrière contenu dans l'article 3 du statut des membres des services extérieurs en vue de permettre leur mobilité vers d'autres services publics, notamment en cas de perte de l'habilitation de sécurité.

[170] Cette durée est normalement de cinq ans selon l'article 26 de l'arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité.

CHAPITRE 5: RAPPORT CONCERNANT L'ENQUÊTE DE CONTRÔLE RELATIVE À LA SÉCURITÉ ET À LA SURVEILLANCE D'UN DÉPÔT MILITAIRE D'ARMES (THUIN)

1. INTRODUCTION

Dans la nuit du 21 au 22 mai 2002, sur le site militaire hennuyer de Thuin dénommé « Le Guibet », deux sentinelles furent d'une manière spectaculaire attaquées et prises momentanément en otage.

A la suite de cette agression trois inconnus se sont enfuis en emportant une grande quantité d'armes de guerre.

Quelques jours plus tard la quasi-totalité des armes dérobées ont été retrouvées par les services judiciaires de l'arrondissement de Charleroi dans un immeuble abandonné de la région et quelques arrestations furent opérées.

2. LE FONDEMENT DE L'ENQUÊTE

Étant donné l'impact des attaques du 11 septembre 2001 et l'éventualité d'un risque de sécurité accru, le Comité permanent R a estimé nécessaire de réaliser une enquête sur les directives applicables en la matière et sur la réaction du SGR/S suite à l'incident de sécurité précité.

Les événements ont suscité aussi bien sur le plan local qu'au niveau fédéral un grand intérêt de la part des médias.

Ils ont donné lieu aux interpellations parlementaires suivantes adressées au Ministre de la Défense nationale :

A. (Question orale) n° 7295 du 23 mai 2002 de Monsieur le Député Ferdy Willems :

Monsieur Willems s'interroge en premier lieu sur l'existence e.a., d'informations préalables adressées aux autorités communales sur la présence d'armes et de munitions sur le site et sur la prise en considération de la sécurité de la population locale.

La question concernant la quantité exacte des armes et munitions volées et sur les éventuelles mesures préventives de sécurité prises en général dans les casernes est également posée.

Le député suggère que l'ensemble de l'armement de l'armée belge fasse l'objet de la part de celle-ci d'un examen critique du point de vue de la sécurité de la population.

B. Question orale n° 7300 du 23 mai 2002 de Monsieur le Député Pieter De Crem :

Monsieur De Crem demande qu'il soit répondu à la question de savoir quel est le service ou l'organisation qui doit exercer un contrôle sur un dépôt d'armes et avec quelle régularité ce contrôle s'effectue-t-il ?

Il est également demandé de préciser quels sont les critères retenus lors de la rédaction des règles de sécurité et si ces directives font l'objet d'une évaluation après chaque incident avec comme corollaire le cas échéant le suivi de telles évaluations.

C. Question orale n° 7315 du 24 mai 2002 de Monsieur le Député Olivier Chastel :

Monsieur Chastel demande si des règles de sécurité sont prises et si on dispose des moyens financiers nécessaires pour améliorer le stockage des armes.

Il est proposé d'envisager une collaboration et un échange de renseignements concernant ces dépôts avec les autorités communales et la police locale. La question est aussi posée d'une suppression des dépôts d'armes décentralisés et moins gardés.

3. PROCÉDURE

Le Comité permanent R a considéré au cours de sa réunion du 31 mai 2002 que le vol d'armes à Thuin était un incident de sécurité grave et il a donné comme mission à son Service d'enquêtes de faire un premier point du cadre de l'enquête et des questions posées.

Par courrier du 14 juin 2002, le Service d'enquêtes a transmis au Président du Comité permanent R les résultats de cette première évaluation et dressait une liste élargie des questions qui se posaient dans le cadre de la préparation de cette enquête.

Ce premier projet a été approuvé le 10 septembre 2002 et une apostille transmise au Service d'enquêtes afin de débuter l'enquête proprement dite relative à la manière dont le SGRS avait suivi l'incident.

Conformément à l'article 43 §1 de la loi organique du 18 juillet 1991, le chef du Service d'enquêtes du Comité R a averti le 5 septembre 2002 le ministre de la Défense nationale de l'ouverture de l'enquête de contrôle.

Le 19 septembre 2002, un questionnaire détaillé a été transmis au SGRS. L'orientation de l'enquête et les premiers résultats de celle-ci furent discutés à l'occasion de deux réunions de travail avec le chef de la division Sécurité du SGRS/S. Le 14 octobre 2002 le Service d'enquêtes a reçu les éléments de réponse.

4. ENQUÊTE PRÉCÉDENTE

A l'occasion d'un vol d'armes dans le dépôt militaire de Houthulst en 1997, le Comité permanent R avait déjà réalisé une enquête approfondie relative à l'application des normes appliquées[171] .

La plus grande partie de ces règles sont toujours d'application actuellement et ne sont pour cette raison que brièvement rappelées ci-dessous.

La plupart des modifications intervenues résultent de la réorganisation fondamentale intervenue au sein des Forces armées et du passage à la « structure d'unités »

5. LES NORMES

Les normes applicables sont toujours celles contenues dans le *'Règlement sur la Sécurité Militaire'* (IF5).

Dans les grandes lignes on peut dire que ce règlement[172] contient la politique de sécurité générale d'application dans les forces armées ainsi que la manière dont cette politique est mise en œuvre.

Le Règlement 'IF5' est complété par le Règlement 'IF5-bis', dans lequel sont déterminées les normes d'infrastructure et les exigences techniques auxquelles les dépôts d'armes et de munitions doivent répondre.

Le Règlement 'IF5-bis' prévoyait déjà des mesures de transition en ce qui concerne la conformité des installations. Ces mesures de transition devaient en principe être applicables jusqu'au 31 décembre 2002.

Il a été communiqué par le SGRS que suite à la restructuration de la Défense Nationale le Règlement 'IF5' sera totalement revu. Par analogie, le règlement 'IF5-bis' sera également soumis à révision.

6. COMPÉTENCES ET RESPONSABILITÉS EN MATIÈRE DE CONTRÔLE DES DÉPÔTS D'ARMES ET DE MUNITIONS

6.1. Modifications subséquentes à la mise en place de la structure unique

Suite à la réforme de la Défense, les diverses composantes militaires ont été supprimées et reprises dans une structure unique. Cela implique e.a. aussi que le commandement territorial inter forces soit supprimé et que l'Unité de Sécurité inter forces qui y était associée soit début 2002 intégrée au SGR-S (division sécurité du SGR).

[171] Voir le Rapport d'Activités 1999 du Comité permanent R, p. 74
[172] cf. Rapport annuel 1999 précité

L'ancienne Unité de Sécurité Inter Forces se dénomme désormais SGRS-S/SU (Security Units) et a conservé ses anciennes compétences. Elle consiste en un commandement et en une série de détachements qui en principe sont organisés à raison d'un détachement pour deux provinces, à l'exception de Liège et du Brabant où à chaque fois un détachement est installé.

Au sein du SGR-S même est également intervenu un changement de dénomination: la dénomination SGRS/SMI est entre-temps devenue SGRS-S/MIS (Military and Industrial Security).

6.2. Responsabilité pour la surveillance et le contrôle

La protection et la surveillance des dépôts et magasins sont placés sous la responsabilité des autorités militaires qui en ont la gestion, à savoir, normalement de commandant de quartier.

Pour cela, il faut tenir compte des Directives de base 'IF5' et 'IF5-bis', mais aussi des circonstances locales pour la prescription de données plus détaillées en de prescriptions, mieux précisées dans le dossier de sécurité du quartier (qui donne en détail la configuration du quartier en ce qui concerne la sécurité) et dans le dossier relatif à la garde qui contient les directives complètes à l'attention du personnel de garde.

6.3. Compétences, contrôles et suivi

6.3.1. Unité / Quartier

Les contrôles sont en première instance exécutés par la hiérarchie locale, via le personnel de l'unité (Commandant de poste, Officier de garde, Capitaine de semaine….).

6.3.2. SGRS-S/SU

La compétence du SGRS-S/SU dans cette matière est principalement par nature celle de conseiller : en premier lieu, conseiller le commandement militaire responsable[173] concernant les mesures de protection qui s'imposent, vérifier leur exécution, constater à l'occasion de celle-ci les lacunes éventuelles et transmettre les manquements constatés au commandement militaire accompagnés des recommandations nécessaires pour y remédier.

SGRS-SU réalise des contrôles sur l'application concrète des prescriptions de sécurité indépendamment des contrôles de la hiérarchie locale ci-dessus mentionnés.

Les tâches générales de contrôle consistent e.a. en une inspection générale de sécurité bisannuelle de tous les quartiers militaires, durant lesquelles les directives de sécurité sont vérifiées et leur mise en oeuvre contrôlée en apportant une attention particulière pour les endroits où des armes sont entreposées.

Cela comporte aussi e.a. des inspections non annoncées et la transmission de rapports écrits de constatations via la voie hiérarchique.

[173] Voir supra rubrique 6.2

6.3.3. SGRS-S /MIS

Quand un incident a une certaine ampleur et qu'il peut avoir des répercussions en dehors du milieu militaire, le SGRS-S/MIS peut effectuer sa propre enquête ou approfondir l'examen réalisé par SGRS-S/SU[174].

6.3.4. Suivi

En fonction des résultats de l'inspection, une ou plusieurs autres contrôles peuvent être réalisés.

Les mesures qui sont prises à la suite de ces rapports dépendent du contexte local et sont fortement dépendantes des moyens disponibles en termes de personnel, de matériel et de budget.

7. PROCÉDURE EN CAS D'INCIDENT

A l'occasion d'un incident survenu dans une installation ou dans une unité militaire l'enquête sur place est effectuée en premier lieu par le SGRS-S/SU[175], et plus spécifiquement la section qui a l'unité concernée sous sa responsabilité.

Si la nature et les conséquences de l'incident sont limités ou ont un caractère local, le SGRS-S/SU appréciera l'enquête et les mesures prises en vue de réaliser des évaluations générales subséquentes.

Si l'incident a au contraire des conséquences telles que des répercussions à l'extérieur de la sphère militaire doivent être envisagées, ou bien lorsque les résultats de l'enquête du SGRS-S/SU doivent être complétés, le SGRS-S/MIS peut approfondir l'enquête ou démarrer ses propres investigations.

Dans le cas du vol de Thuin, le Service d'enquêtes du Comité R a pu constater sur la base des données qui lui ont été communiquées par le SGRS-S que les procédures prévues ont été respectées (avertissement et rapports d'urgence).

Vu le caractère sérieux de la situation, le dossier a été immédiatement suivi de près par le SGRS-S et diverses initiatives ont été prises pour anticiper la survenance de nouveaux incidents du même type dans l'avenir (cf. infra).

8. VOL COMMIS DANS LE QUARTIER « LE GUIBET » À THUIN

8.1. Faits concrets

Le 22 mai 2002, à environ 00.10 heures, trois individus masqués et armés pénètrent dans le quartier militaire après avoir sectionné la clôture située à l'arrière du poste de garde.

[174] Voir infra rubrique 7
[175] Les compétences en la matière de ce service sont décrites dans le Règlement 'IF5'- Chapitre 1 §104

Ils ont d'abord neutralisé la sentinelle maître-chien au moment ou celle-ci terminait sa ronde après avoir ramené son chien dans sa niche. Ensuite, ils ont maîtrisé la deuxième sentinelle par surprise dans le local de garde. Les deux gardes furent attachés et bâillonnés.

Après avoir tenté de forcer le dépôt d'armes ils ont forcé le personnel de garde à leur remettre toutes les clefs. Comme malgré tout cela ils ne parvenaient pas à ouvrir le magasin, ils ont obligé, sous la menace, le personnel de le faire.

Finalement, les assaillants ont emporté avec eux la plus grande partie des armes de l'unité, à savoir :

- 130 fusils FNC + chargeurs ;
- 14 pistolets GP ;
- 50 chargeurs pour fusil FNC ;
- 1 paire de jumelles.

De surcroît, les munitions suivantes ont été dérobées dans le local de garde :

- 40 cartouches 5,56 mm ;
- 10 cartouches 9 mm.

Les agresseurs ont pris la fuite avec le véhicule personnel d'un des gardes en abandonnant les deux militaires ligotés à l'arrière du magasin d'armes. Après leur départ, les gardes ont pu assez rapidement alerter la police.

8.2. Renseignements complémentaires

Le quartier « Le Guibet » était occupé par la 100ème compagnie de ravitaillement du 8ème bataillon logistique.

Le quartier comprend à l'instar de tous les quartiers militaires un magasin d'armes et un dépôt séparé pour les munitions légères. Il ne faut donc pas le considérer comme un « dépôt de munitions » au sens strict du terme ; ces derniers sont moins nombreux et ont en fonction de leur mission une plus grande importance et une plus grande capacité de stockage.

Les autorités militaires insistent sur le fait que depuis 1990 des investissements importants ont été faits pour adapter tous les magasins d'armes et les dépôts de munitions aux normes renforcées de sécurité.

Une distinction doit être faite à ce sujet entre les bâtiments existants (anciens) et les constructions récentes, en ce sens que ces dernières satisfont aux normes de sécurité déterminées dans les Règlements 'IF5' et 'IF5-bis'.

Il a donc été tenu compte pour les anciens bâtiments, au moment de la rédaction des règlements 'IF5' et 'IF5-bis', d'une période transitoire devant se terminer le 1er janvier 2003.

Durant cette période transitoire des locaux ont été utilisés qui n'étaient pas conformes, mais qui avaient subis des adaptations partielles.

La caserne de Thuin est dans ce sens un cas particulier, parce que le quartier fut de fait, temporairement occupé par une unité qui attendait une affectation définitive : d'abord à Ath, ensuite à Tournai et actuellement à Baronville.

Ces incertitudes ont été déterminantes dans le défaut d'investissements importants et spécifiques.

8.3. Inspection(s) par le SGRS-S/SU à Thuin

Selon les informations communiquées par le SGRS-S et les rapports rédigés à ce sujet, il ressort que la dernière inspection effectuée par le SGRS-S /SU (agissant encore à cette époque sous la dénomination :Unité de Sécurité Inter Forces)[176] concernant les mesures de sécurité d'application à Thuin date du 12 avril 2001.

Diverses observations furent à l'occasion formulées par les contrôleurs - e.a. en ce qui concerne la sécurité des armes - principalement par référence aux procédures prévues par le règlement IF 5, mais aussi en ce qui concerne les serrures et la conservation des clefs.

Les constatations furent adressées dans une note du 23 avril 2001 respectivement aux commandants d'unité et de bataillon ainsi que pour information au commandant de province, au commandant de la division logistique et au commandant SGR/SMI.

Dans une note datée du 17 mai 2001 le Commandant d'unité communique les modifications aussi bien organisationnelles que structurelles qui ont été décidées et /ou réalisées après le contrôle du 12 avril 2001, pour rencontrer les observations formulées par les contrôleurs.

8.4. Incidents de sécurité antérieurs au vol d'armes de Thuin

Au cours de l'enquête, qui a suivi le vol, il est apparu que dans la période précédant celui-ci la clôture d'enceinte du quartier avait été endommagée.

En premier lieu, on a pensé qu'il pouvait s'agir de membres du personnel qui avaient de cette manière fait passer frauduleusement du matériel à l'extérieur (quelques faits de vols et de détournement de matériel de cette nature avaient en effet été constatés).

En plus de la réparation immédiate de la clôture des mesures draconiennes de sécurité furent prises par le commandant d'unité, comme des contrôles inopinés, des vérifications des coffres de voitures, l'exécution d'un certain nombre de rondes extérieures et un contrôle renforcé sur le personnel de garde….

Toutes les mesures furent consignées dans des notes de service contenant des instructions spécifiques à destination des officiers de service et du personnel de surveillance.

Les incidents furent à chaque fois signalés à la hiérarchie compétente et au commandant du SGRS-S/SU.

[176] Cf. remarque ad hoc - rubrique 6.1

9. LES RÉACTIONS SUITE AU VOL D'ARMES

9.1. Du Commandant de quartier et des autorités militaires compétentes

Le jour même du vol, toutes les mesures d'alerte prévues par le Règlement 'IF5' mises en œuvre et une commission d'enquêtes fut mise sur pied au sein du corps.

Les mesures de sécurité furent encore renforcées et les armes restantes furent transportées vers un autre quartier où une meilleure surveillance était garantie.

Des contacts furent pris avec les autres compagnies du bataillon pour prendre des mesures communes.

9.2. Du SGRS-S

La nuit même du vol, une enquête fut initiée par le SGRS-S/SU. Le jour même, un avis urgent fut rédigé et diffusé à tous les quartiers militaires et à toutes les unités annonçant l'incident et demandant à tous les commandants de quartiers et/ou d'unités de porter une attention particulière à la sécurité des magasins d'armes et de munitions et d'appliquer de manière stricte les dispositions du Règlement 'IF5'.

9.3. Du Ministre de la Défense nationale

En réponse à une question parlementaire relative au vol d'armes, il a été répondu que suite à cet incident de sécurité, les mesures suivantes ont été prises :

- faire l'inventaire des lieux d'entreposage des armes et des munitions ;
- vérifier si les infrastructures répondaient aux conditions de sécurité ;
- le cas échéant, si nécessaire et pour autant que la situation le permette, procéder au regroupement des endroits de stockage des armes et munitions ;
- si nécessaire, libérer des moyens financiers pour l'exécution de travaux d'infrastructures urgents et indispensables.

Il a déjà été signalé qu'à côté des mesures ponctuelles déjà évoquées, le ministère de la défense nationale étudierait de manière plus générale la problématique de la surveillance des quartiers et procéderait à une réévaluation de l'infrastructure des endroits où des armes et munitions étaient stockées (des propositions concrètes étaient attendues pour la fin juin 2002).

10. L'ENQUÊTE GÉNÉRALE SUR LES DÉPÔTS D'ARMES ET DE MUNITIONS

10.1. Réaction à propos de l'incident

Le jour même de l'incident de sécurité, une enquête a été ordonnée au sein de la défense et sur ordre du 'CHOD' (Chief of Defense) afin ;

- d'enregistrer un certain nombre de magasins d'armes existant au sein de la Défense nationale;
- de contrôler quels étaient les dépôts conformes aux prescriptions du Règlement 'IF5-bis' ;
- de rechercher dans quelle mesure les magasins d'armes pouvaient être regroupés ;
- d'établir quels dépôts pouvaient être supprimés.

10.2. Les suites de l'incident

Dans un premier stade, le SGRS a dressé un inventaire des dépôts existants et a vérifié dans quelle mesure ils étaient conformes au Règlement 'IF5-bis'.

Le résultat de cette enquête a montré qu'environ la moitié seulement des dépôts d'armes satisfaisait aux normes les plus strictes du Règlement précité. Dans ceux qui n'étaient pas conformes, certains étaient vide et une dizaine pouvaient être rendus conformes après de petites adaptations.

La plus grande majorité des dépôts non conformes (des anciennes installations) nécessitait des travaux conséquents ou des transferts dans des installations adaptées (la plupart du temps ces transferts étaient déjà prévus ou planifiés, mais pas encore réalisés).

Comme cela a déjà été signalé plus haut[177], une phase transitoire avec des mesures temporaires était déjà prévue dans le Règlement 'IF5-bis' (Chapitre 4) pour les installations non conformes.

Cette phase transitoire - qui rencontre partiellement la réorganisation plus importante qui est celle du passage à « la structure unique » - se terminait à la fin 2002, date à laquelle les magasins de stockage des armes devaient répondre aux normes de sécurité.

L'étude du regroupement de ces installations a un très grand impact sur l'ensemble des forces armées et elle tombe par conséquent en dehors du champ de compétence du SGRS.

L'étude a été transmise pour suite utile au CHOD (Chief of Defense).

[177] Voir supra rubrique 8.2

Actuellement, c'est le ACOS (Assistant Chief of Staff) Ops et Trg (Operations & Training) qui est chargé d'approfondir l'étude initiale faite par le SGRS.

11. L'ENQUÊTE JUDICIAIRE ET LA COOPÉRATION AVEC LES SERVICES EXTÉRIEURS

11.1. L'enquête judiciaire

Les constatations initiales ont été faites par la police locale de Thuin. L'Auditeur militaire fut informé des événements.

L'enquête judiciaire subséquente fut reprise par la Police fédérale de Charleroi, section Banditisme en collaboration avec des membres du Détachement judiciaire.

Le 30 juillet 2002, un adjudant de l'unité (en service au secrétariat) a été emmené pour interrogatoire. Il a avoué aux enquêteurs judiciaires qu'il avait communiqué des informations qui avaient été utiles pour la préparation de l'attaque. Suite à ces déclarations, l'intéressé a été immédiatement mis à pied pour une période minimum de trois mois.

Le SGRS a décidé pour sa part le retrait immédiat de l'habilitation de sécurité de l'intéressé. Celui-ci était titulaire d'une habilitation du niveau « secret », délivrée le 24 janvier 2000 et valable en principe jusqu'au 24 janvier 2005.

La notification de ce retrait fut faite par écrit à l'officier de sécurité du 8ème Bat. Log le 2 août 2002.

11.2. La coopération avec les services de police

La collaboration avec les services de police s'est déroulée de manière continue ; des contacts réguliers ont eu lieu entre l'Unité, le SGRS et le service de police chargé de l'enquête. Des informations ont été échangées dans la mesure cependant où cet échange ne nuisait pas à l'enquête judiciaire.

11.3. La Sûreté de l'État

Les services de la Sûreté de l'État ne furent pas informés par le SGRS de l'incident. Les informations subséquentes en rapport avec le dossier ont seulement été échangées avec les autorités judiciaires responsables (la Police fédérale - le Direction judiciaire de Charleroi et l'Auditeur militaire.)

12. CONSTATATIONS DU COMITÉ PERMANENT R

Sur la base des éléments fournis par le SGRS/S, il peut être conclu que dans le cadre de l'incident de sécurité dont question, les procédures prévues par le Règlement 'IF5' ont été suivies.

Le SGRS - dans le cadre de ses compétences et de ses moyens dans ce domaine - a rempli sa mission en conformité avec les procédures.

Comme cela a été souligné par le SGRS-S, il faut d'autre part constater que les installations des forces armées ne sont pas toujours conformes aux prescriptions techniques déterminées dans le règlement susdit, et que l'on peut craindre – maintenant que la période de transition est échue depuis la fin 2002 - de se trouver en présence d'un problème de sécurité.

Dans le cas de Thuin, il est spécifique qu'il s'agit d'un corps qui ne dispose pas encore d'une localisation fixe - ce qui devait être le cas fin 2002 - et qui de surcroît, comme cela avait déjà été constaté par le SGRS, avait à sa disposition un dépôt d'armes non conforme.

Cette problématique de sécurité a été rencontrée d'une certaine manière par la restructuration de la Défense nationale, avec e.a. des conséquences importantes concernant l'occupation des sites et les problèmes logistiques connexes; le problème de la sécurité des dépôts d'armes et de munitions étaient à l'agenda et les événements de Thuin l'ont d'une manière ou d'une autre rendu plus urgent.

La commission d'enquête créée à la suite de l'incident de sécurité indique dans les conclusions de son rapport final, qu'il doit être évité que le personnel de garde dispose des clés ou des codes donnant accès au magasins d'armes et qu'en fin de compte, seul l'armurier et l'officier S2/S3 devraient en disposer.

Vérification faite auprès du SGRS, il apparaît clairement que cette problématique se pose et qu'elle a été évaluée déjà à diverses reprises sous ses différentes facettes, mais qu'aussi bien sur le plan de la sécurité, tant physique que matérielle, il y a des arguments pour et contre à formuler concernant une telle réglementation. Il est de toute manière évident qu'il n'y a en la matière aucune directive ou procédure formelle contraignante.

Dans le cadre de ce dossier, l'enquête de sécurité du membre du personnel impliqué[178] a été vérifiée par le service d'Enquêtes R, parce qu'il avait été constaté aussi bien dans le contexte de l'enquête de corps que de l'enquête judiciaire que l'intéressé aurait connu des problèmes de boisson et des problèmes financiers.

La commission d'enquête précitée (qui a réalisé l'enquête de corps), formulait déjà l'opinion que *'l'habilitation de sécurité de quelqu'un qui avait de grave problèmes de boissons, devait être, même temporairement retirée'.*

Dans le dossier de l'enquête de sécurité de l'intéressé aucune pièce n'a été trouvée qui indiquait le moindre problème en relation avec l'alcool. Il était constaté que l'intéressé avait toujours eu des états de service irréprochables et que son comportement ne justifiait aucune remarque.

[178] Voir supra, point 11.1

Ce n'était que récemment, par une note du 20 février 2002, que le service financier de la Défense nationale signalait une saisie sur salaire faisant suite au non-remboursement d'un prêt personnel. Cet élément fut ajouté dans le dossier de sécurité, mais n'a visiblement pas donné lieu à une vérification ou à une révision quelconque.

Dans une enquête similaire relative au vol d'armes dans un dépôt militaire à Houthulst en 1997, le Comité permanent R avait déjà formulé la recommandation de prévoir une enquête de sécurité pour les membres du personnel en mission dans des zones protégées. La loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité permet aujourd'hui de régler ce problème.

A l'époque la suggestion avait également été faite d'organiser une collaboration avec la police locale et avec les autorités civiles locales, afin de pouvoir intervenir de manière rapide et coordonnée en cas de survenance d'incidents de sécurité.

Les questions parlementaires à ce sujet montrent clairement que la population et les autorités civiles souhaitent - de préférence de manière anticipative- être informées de risques éventuels.

13. DONNÉES SUPPLÉMENTAIRES

En relation avec les recommandations ci-dessus rappelées d'effort de coordination et de coopération entre les autorités militaire et civile, le Comité permanent R a posé une question complémentaire en rapport avec les déclarations faites par Nizar TRABELSI relatives à la commission d'un attentat éventuel ayant comme cible la base de Kleine-Brogel.

Cette question était ainsi formulée :

« Dans votre rapport concernant l'agression commise au dépôt d'armes de Thuin, il est fait notamment référence d'une part à une étude du SGRS ayant pour sujet la sécurité des installations militaires et d'autre part aux résultats d'une enquête sur l'application des nouvelles normes (règlement IF5-bis).

Vu les compétences et les mission du SGRS en la matière, il semble opportun de savoir de quelle manière le SGRS a été informé des déclarations faites par Trabelsi ayant trait à un éventuel attentat visant la base de Kleine-Brogel.

Il semblerait : que cette information ait été disponible avant le 11 septembre 2001; que Trabelsi aurait donné des détails accréditant ses déclarations concernant un attentat ; qu'il aurait expliquer le choix de Kleine-Brogel «parce que cette base n'était pas bien surveillée».

Voudriez-vous vérifier de quelles informations le SGRS disposait, comment ces informations ont été traitées et éventuellement rapportées?».

Dans sa réponse, le SGRS indique que ce service n'a jamais été informé par le juge d'instruction et qu'il n'a eu connaissance des déclarations dont question ci-dessus que via la presse.

Il ne s'agissait pas ici d'un oubli mais d'un embargo imposé par le juge d'instruction et cela malgré le demande et les échanges de vue avec le Magistrat fédéral. En ce qui concerne l'affirmation selon laquelle la base de Kleine-Brogel serait «mal surveillée», il est signalé que le sécurité est conforme aux normes applicables en Belgique et à l'OTAN.

14. CONCLUSION

Le SGRS a suivi l'incident de manière adéquate compte tenu de ses nouvelles compétences. Il ne s'en est pas tenu au seul incident de Thuin. Un inventaire a été réalisé des magasins existant et il a été examiné dans quelle mesure ceux-ci étaient en conformité avec le prescrit réglementaire.

Il convient de constater que la coopération entre les différents services devrait encore être améliorée.

CHAPITRE 6: RAPPORT SUR L'INTERET QU'ONT PORTE LES SERVICES DE RENSEIGNEMENT A UN VOL DE DONNEES SENSIBLES COMMIS DANS UNE SOCIETE COMMERCIALE BELGE FOURNISSANT DES PRODUITS ET SERVICES DE HAUTES TECHNOLOGIES

1. INTRODUCTION

Suite à des informations transmises au Comité permanent R à propos d'un vol d'ordinateurs commis en mai 2002 au siège d'une firme X installée dans un parc scientifique, deux membres du Comité permanent R se sont rendus le 3 juillet 2002 au siège de cette société afin d'y rencontrer ses responsables et d'en apprendre davantage sur les circonstances et les objectifs de ce vol.

Les voleurs semblent avoir agi en véritables professionnels au regard du modus operandi puisqu'ils ont réussi à neutraliser le système d'alarme par détection infrarouge. Manifestement, c'était le contenu des ordinateurs (le disque dur) de cette firme qu'avaient visé les voleurs et non l'appareillage lui-même puisqu'ils ont négligé du matériel d'une valeur commerciale certaine. Les disques durs emportés contenaient, en effet, des données sensibles, des analyses et des informations exclusives destinées aux clients civils de l'entreprise. L'information ainsi dérobée représentait une valeur commerciale importante, susceptible d'être aussi utilisée à des fins militaires. La Sûreté de l'Etat avait été prévenue du vol, mais pas le SGR.

La société concernée est une spin-off, c'est-à-dire une entreprise créée dans le sillage d'un centre de recherche scientifique universitaire dont elle exploite commercialement les applications scientifiques qui y ont été mises au point. Les produits et services développés par la firme en question mettent en œuvre une technologie avancée et s'adressent principalement aux secteurs civil et humanitaire. Toutefois, ils sont aussi susceptibles d'intéresser les militaires. Le Comité permanent R a ainsi appris que des militaires, probablement membres du SGRS, avaient pris contact dans un passé récent avec les responsables de la firme.

A peu près à la même époque que ce vol, d'autres firmes établies sur le même parc scientifique ont aussi été les victimes de cambriolages de même nature. En novembre 2002, la firme X fit encore l'objet d'une tentative de vol, infructueuse cette fois. Ces cambriolages n'ont fort heureusement pas eu de conséquences négatives sur les contrats, ni sur la qualité des relations que la firme X entretient avec ses clients. Ses responsables souhaitent néanmoins qu'il ne soit pas donné de publicité inutile à propos de ces incidents.

La firme X ne semble pas être la seule à subir de telles mésaventures puisqu'en décembre 2002, la presse a relaté une autre vague de vols d'ordinateurs dans plusieurs entreprises établies dans la province de Flandre occidentale [179]..

[179] « De Standaard » - 26 décembre 2002

Cette situation n'est pas sans rappeler les circonstances qui ont donné lieu à l'enquête du Comité permanent R « *sur la manière dont les services de renseignement ont réagi à propos d'éventuels faits d'espionnage ou de tentative d'intrusion dans le système informatique d'un centre de recherche belge* » [180].

Le Comité permanent R a dès lors estimé que les faits ainsi rapportés contenaient à nouveau des indices d'espionnage susceptible de porter atteinte au potentiel scientifique et économique du pays. Il s'est donc demandé comment la Sûreté de l'Etat avait réagi face à cette situation. Le Comité permanent R s'est aussi interrogé sur l'intérêt que le SGRS avait naguère porté à la firme concernée par ce vol d'ordinateurs.

2. PROCEDURE

Suite à ces constatations et à ces interrogations, le Comité permanent R a pris la décision d'ouvrir la présente enquête de contrôle le 3 juillet 2002.

Le Service d'enquêtes R fut chargé le même jour de procéder à diverses investigations.

Le président du Sénat et les ministres compétents en furent avertis le 4 juillet 2002.

Le Service d'enquêtes R a mené son enquête au cours des mois d'août et de novembre 2002. Il a déposé son rapport le 18 décembre 2002. Ce rapport est classifié confidentiel au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité en raison de l'atteinte qu'une utilisation inappropriée de ce document pourrait porter au potentiel scientifique et économique de l'entreprise concernée.

Le Comité permanent R a approuvé le présent rapport destiné au Parlement le 16 janvier 2003.

Il est revêtu de la mention « diffusion restreinte » en application de l'article 20 de l'arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité.

3. CONSTATATIONS

3.1. L'intérêt porté à la firme X par le SGRS.

Pour rappel, lors de leur visite à la firme X en juillet 2002, les membres du Comité permanent R avaient notamment appris que deux militaires belges, appartenant probablement au SGRS, avaient eu des contacts avec les responsables de la société. Ce point ainsi que les noms des deux officiers firent donc l'objet de questions adressées au chef du SGRS.

Les circonstances qui amenèrent le SGRS à connaître et à s'intéresser à la firme X furent précisées dans une réponse écrite de ce service, datée du 5 août 2002. Cette lettre était accompagnée de diverses pièces annexes.

---

[180] Voir rapports d'activités 2000 : p. 60 (Fr) – p .62 (Nl) et suivantes et 2001 : p. 68 (Fr) – p .74 (Nl) et suivantes.

Se référant à ces diverses pièces transmises, il appert qu'il y eut effectivement deux rencontres entre des membres du SGRS et des responsables de la firme X. Une première fois lors d'une présentation générale des produits et services de la firme effectuée en avril 2001 au cabinet du Ministère de la Défense nationale, et une seconde fois, lorsque deux membres du SGRS, présents à cette démonstration, se sont eux-mêmes rendus quelques jours par après dans les locaux de la firme X afin d'y recevoir un briefing plus détaillé sur le plan technique.

Les relations entre le SGRS et la firme X peuvent être retracées de la façon suivante :

- en mars 2001, le Ministère de la Défense nationale a reçu les représentants de la firme X, désireux de lui faire connaître leurs services et produits ;

- sur base des fascicules transmis par la firme elle-même, le secrétariat administratif et technique du ministère de la Défense nationale demanda au SGRS de se prononcer sur l'intérêt éventuel des produits présentés pour les forces armées belges et ce, en vue de préparer une nouvelle réunion d'évaluation au cabinet de la Défense, réunion à laquelle le SGRS était par ailleurs prié d'être représenté. A l'issue de cette réunion, il fut convenu qu'une réunion ultérieure complémentaire et plus technique se tiendrait ultérieurement au siège de la société X ;

- suite à cette nouvelle rencontre, un membre du SGRS a rédigé un rapport exprimant ses commentaires positifs au sujet des produits et services proposés par la firme. Ce rapport fut adressé au cabinet du Ministère de la Défense nationale. Plus aucun contact ultérieur n'a été établi entre le SGRS et la firme X.

- Le SGRS a par ailleurs précisé que la firme X n'était pas connue jusqu'alors de ce service et qu'elle n'était pas davantage titulaire d'une habilitation de sécurité.

- En décembre 2002, un responsable du SGRS a confirmé ne pas avoir été mis au courant des vols de matériel informatique commis en mai 2002 au préjudice de cette société et n'avoir jamais été chargé de devoirs spécifiques dans ce cadre.

3.2. L'intérêt porté à la firme X par la Sûreté de l'Etat

La Sûreté de l'Etat a répondu aux questions posées par le Comité permanent R le 6 août 2002. Cinq documents internes concernant directement ou indirectement la société X accompagnaient cette réponse. Il s'agit des cinq rapports établis entre les mois de juin et novembre 2002.

Il en ressort que le vol dont la firme X a été la victime au mois de mai 2002 avait été porté à la connaissance de la Sûreté de l'Etat peu de temps après ces faits. Le SGRS a également informé la Sûreté de l'Etat de nouvelles tentatives d'intrusions informatiques contre un centre de recherche Y établi dans le même parc scientifique.

Les relations entre la Sûreté de l'Etat et la firme X peuvent être retracées de la façon suivante :

- un premier rapport établi en juin 2002 fait état de la fréquence des vols et des attaques informatiques à l'encontre des établissements établis dans le parc scientifique Z où la firme X et le centre de recherche Y sont installés. Ce rapport indique que des mesures de sécurité ont été prises ;

- un second rapport rédigé le même mois concerne le vol commis à l'encontre de la firme X en particulier. Il en décrit l'objet, les circonstances et le modus operandi ;

- une apostille rédigée début juillet 2002 charge le bureau local de la Sûreté de l'Etat d'enquêter sur place au sujet des mesures de sécurité prises dans le parc scientifique concerné, d'identifier qui serait susceptible d'être intéressé par les produits et matériels développés dans ce parc et d'examiner s'il existe des normes internationales en vue de la sécurisation de ces produits ;

- une seconde apostille rédigée en juillet 2002 fait suite à l'information reçue du SGRS concernant les tentatives d'intrusions dans le système informatique du centre de recherche Y ;

- le troisième rapport rédigé en août 2002 suite à la première apostille précitée mentionne la prise de conscience croissante des responsables des spin-off du parc Z à la protection de leur potentiel scientifique et économique, situation qui se traduit par la mise en place d'une « *coordination de type privé afin de mieux assurer la sécurité du site* ». Ces mesures de sécurité sont renforcées par le travail de la Police Fédérale qui multiplie les patrouilles et entretient des contacts avec les firmes de gardiennage présentes sur le site. Et le rapport de conclure : « *la mobilisation plus accrue de la Police Fédérale autour du site Y est récente et, semble-t-il, en partie due à l'intérêt porté par la Sûreté de l'Etat à la protection du potentiel économique et scientifique dans la région* ». Les promoteurs du parc Z ont d'ailleurs interpellé les autorités à ce sujet ;

- un quatrième rapport de novembre 2002 décrit les mesures prises par la firme X destinées au renforcement de sa sécurité après la tentative de vol dont elle a été la victime au cours de ce mois.

La Sûreté de l'Etat indique par ailleurs que ses services poursuivent leurs investigations à propos des vulnérabilités apparues dans les firmes et centres de recherches concernés, notamment par la prospection et la sensibilisation des autorités locales et des chefs d'entreprises. La Sûreté de l'Etat cherche aussi à cerner le profil des auteurs des vols informatiques et leur motivation alors que l'hypothèse privilégiée de la police locale est celle de vols destinés à obtenir du matériel informatique, sans égard pour le contenu des disques durs. Ces vols seraient facilités par la configuration particulière des lieux. Les responsables de la firme X n'ont par ailleurs pas décelé la moindre tentative d'intrusion dans leur système informatique.

Le service d'enquête précise également que, sur le terrain, aucun échange particulier d'information n'a eu lieu entre les antennes locales de la Sûreté de l'Etat et du SGRS.

4. CONCLUSIONS

- jusqu'en 2001, la société X ne faisait l'objet d'aucune attention particulière de la part de la Sûreté de l'Etat ni du Service Général de Renseignement et de Sécurité ;

- le SGRS est entré en relation avec la firme X au printemps 2001 en vue de satisfaire la demande du Ministre de la Défense nationale d'évaluer l'intérêt éventuel des produits et services que la firme en question avait pris l'initiative de proposer aux forces armées belges. Un rapport a été adressé au Ministre. Il n'y a pas eu d'autre suivi ;

- la Sûreté de l'Etat a quant à elle été rapidement mise au courant du vol d'ordinateurs perpétré à l'encontre de la firme X. Elle a aussi été mise au courant par le SGRS de tentatives d'intrusions informatiques contre un centre de recherche Y établi dans le même parc scientifique ;

- la Sûreté de l'Etat a, fort opportunément, réagi à ces informations en entamant des investigations à propos des vulnérabilités apparues dans ces firmes et centres de recherches, notamment en prospectant et en sensibilisant les autorités locales et les chefs d'entreprises concernés. La Sûreté de l'Etat n'exclut pas des actes d'espionnage bien que l'hypothèse privilégiée par la police locale soit celle de vols destinés à obtenir du matériel informatique, sans égard pour le contenu des disques durs. La Sûreté de l'Etat cherche donc à cerner le profil des auteurs des vols informatiques ainsi que leur motivation ;

- aucun échange particulier d'information n'a eu lieu entre les antennes locales de la Sûreté de l'Etat et du SGRS ;

- la récente mobilisation plus accrue de la Police Fédérale en vue d'assurer la sécurité du parc scientifique Y est, semble-t-il, en partie due à l'intérêt porté par la Sûreté de l'Etat à la protection du potentiel économique et scientifique dans la région.

5. RECOMMANDATIONS

- le Comité permanent R se réjouit des initiatives prises en la matière par la Sûreté de l'Etat et lui recommande de les mener à terme puisque l'une de ses missions légales consiste à se préoccuper de la protection du potentiel scientifique et économique du pays ;

- le Comité permanent R recommande à la Sûreté de l'Etat de poursuivre cette enquête sur cette affaire en la mettant en rapport avec d'autres cas de vols d'ordinateurs ou d'intrusions informatiques commis au préjudice d'autres entreprises de haute technologie, tant au Nord qu'au Sud du pays ;

- le Comité permanent R est d'avis que la Sûreté de l'Etat doit poursuivre ses investigations dans ces affaires en n'écartant pas l'hypothèse de vols d'ordinateurs commis à des fins d'espionnage économique, voire même militaire. Et quel qu'en soit le mobile, le vol d'ordinateurs contenant des données économiques sensibles représente en soi une atteinte au potentiel économique du pays ;

- le Comité permanent R recommande par conséquent à la Sûreté de l'Etat de poursuivre ses visites auprès des autorités locales et des chefs d'entreprises afin de les sensibiliser à la sécurisation de leur potentiel scientifique et économique. Il recommande aussi une bonne collaboration sur ce sujet avec le cas échéant, le SGRS, les autorités judiciaires, le parquet fédéral et les corps de police locale ;

- le Comité permanent R recommande à nouveau que la Sûreté de l'Etat s'adresse au Comité ministériel du renseignement et de la sécurité pour obtenir les directives nécessaires pour définir le potentiel scientifique et économique que ce service doit protéger ainsi que le prescrit l'article 7, 1° de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

CHAPITRE 7: RAPPORT DE L'ENQUETE DE CONTROLE SUR L'INTERVENTION DES SERVICES DE RENSEIGNEMENT DANS UN CAS DE DISPARITION INQUIÉTANTE D'UNE PERSONNE TRAVAILLANT DANS UN SECTEUR LIE À LA DEFENSE NATIONALE

1. PROCEDURE

Le 2 septembre 2002, le Comité permanent R a été mis en possession de documents relatifs à la disparition d'une personne travaillant dans un secteur stratégique lié à la Défense nationale.

Ces documents furent communiqués, à toutes fins utiles, au Parquet fédéral par courrier du 20 septembre 2002.

Par courrier du 30 septembre 2002, le Parquet fédéral accusait réception de cet envoi et signalait que les documents envoyés n'apportaient aucune information complémentaire.

Lors de sa réunion du 30 septembre 2002, le Comité permanent R a décidé de l'ouverture de la présente enquête de contrôle, certains des éléments communiqués indiquant qu'il pouvait y avoir des aspects de l'affaire touchant au domaine du renseignement et de la sécurité.

Le Président du Sénat a été informé de l'ouverture de l'enquête par courrier du 7 octobre 2002 en application de l'article 32 de la loi du loi organique du contrôle des services de renseignement du 18 juillet 1991.

Les ministres de la Justice et de la Défense nationale en ont été avertis le 14 octobre 2002, en application de l'article 43.1 de la loi du 18 juillet 1991.

Le présent rapport a été approuvé par le Comité permanent R lors de sa réunion du 16 mars 2004.

2. LES OBJECTIFS DE L'ENQUETE DE CONTRÔLE

Compte tenu du fait que la disparition suspecte concernait une personne travaillant dans une entreprise d'un secteur stratégique, le Comité permanent R désirait vérifier :

- Si l'intéressé était connu d'une manière ou d'une autre par la Sûreté de l'Etat et par le SGRS ?

- Si l'entreprise qui n'est pas sans intérêt sur le plan du potentiel économique, ainsi que sur le plan de la Défense nationale, avait des contacts avec les deux services ?

- Si les services de renseignement et de sécurité étaient intervenus dans le cadre d'enquêtes de sécurité en rapport avec l'entreprise, son personnel et la personne disparue ?

- Si les services de renseignement avaient été informés de cette disparition suspecte, et si oui à quel moment ?

- S'il y avait une coopération entre services de police et de renseignement dans cette affaire et le cas échéant comment se déroulait cette coopération ?

3. LES RESULTATS DE L'ENQUETE DE CONTRÔLE

3.1. L'aspect de la sécurité

A. Le SGRS

L'entreprise étant titulaire d'une habilitation de sécurité délivrée par le SGRS, ce dernier service porte un intérêt particulier à la firme ainsi qu'au personnel habilité travaillant sur des projets classifiés.

Si le service a donc bien effectué une enquête de sécurité pour l'entreprise concernée, il n'a pas effectué d'enquête de même nature pour la personne en question qui n'était pas aux dires de son employeur, impliquée dans des programmes classifiés ou dans des projets sensibles.

Le SGRS a été informé, par la police fédérale, le lendemain de la disparition.

Ce service se dit concerné dans le cadre de cette disparition, non seulement par les aspects en relation avec les « habilitations de sécurité », mais également par d'autres faits de vol de matériel informatique intervenus à différents endroits au cours d'une période précédant l'entrée en fonction de la personne disparue, voire d'activités d'espionnage.

Suite à ces événements, le SGRS a effectué une visite de contrôle dans l'entreprise.
Ce contrôle a amené la constatation de certains manquements et incidents de sécurité, concernant notamment la personne disparue.

Suite à ce contrôle et à ces constatations, le SGRS a estimé qu'une mise au point avec l'officier de sécurité était nécessaire dans le cadre d'une sensibilisation accrue aux risques de sécurité inhérent à ce type d'entreprise.

B. La Sûreté de l'Etat

Un peu plus d'un mois après la disparition de la personne concernée, la Sûreté de l'Etat en a été informée par le SGRS à l'occasion d'une concertation bilatérale en matière d'enquêtes de sécurité.

Pour le surplus, la Sûreté de l'Etat n'a jamais effectué la moindre enquête de sécurité pour le compte de l'entreprise concernée.

Suite à l'information reçue, la section de la Sûreté de l'Etat compétente en matière de protection du potentiel scientifique et économique a pris contact avec le SGRS.

La Sûreté de l'Etat souligne que le monde industriel se montre particulièrement circonspect dans ce genre d'affaire et ce, eu égard à son inquiétude vis-à-vis d'atteintes éventuelles à son image de marque.

3.2. La coopération entre les services

A. Le SGRS

Ce service a été informé de la disparition par la police fédérale.

Le SGRS a ensuite travaillé d'après ses dires en étroite collaboration avec le magistrat instructeur. Ce service a même été chargé d'une partie de l'enquête.

B. La Sûreté de l'Etat

Après avoir été informée de la disparition, la Sûreté de l'Etat a rédigé un premier rapport opérationnel, à la suite d'un contact avec la police fédérale. La Sûreté de l'Etat a poursuivi ses investigations dans le cadre de l'enquête judiciaire.

4. CONSTATATIONS DU COMITE R

4.1. Le Comité permanent R constate que c'est suite à la disparition inquiétante d'un membre du personnel de l'entreprise que le SGRS y a décelé certains problèmes de sécurité

4.2. Le Comité permanent R estime qu'à ce niveau un meilleur suivi des problèmes de sécurité pouvant toucher une entreprise titulaire d'une habilitation de sécurité aurait dû permettre de mettre à jour plus rapidement ces manquements de sécurité ; le Comité permanent R souligne toutefois que nonobstant cette constatation le SGRS, une fois informé, a bien réagi en insistant sur le respect des règles élémentaires de sécurité et en effectuant une mise au point avec l'officier de sécurité

4.3. Le Comité permanent R constate que lors d'une enquête de contrôle précédente « sur la manière dont les services de renseignement ont réagi à propos d'éventuels faits d'espionnage ou de tentative d'intrusion dans le système informatique d'un centre de recherche belge » (rapport d'activités 2000 – p. 60), le SGRS, à propos du manque de suivi d'un incident de sécurité, avait justifié son absence d'intervention par le manque de moyens humains qualifié dont il dispose pour effectuer des contrôles réguliers dans des entreprises protégées.

4.4. Le Comité permanent R relève également dans le présent dossier certaines lacunes inhérentes au fonctionnement interne du système de sécurité de l'entreprise, notamment dans le retard mis pour informer le SGRS des incidents de sécurité. C'est ainsi par exemple, qu'un incident grave n'a été communiqué par note au SGRS qu'un mois après les faits.

Sans doute, cela illustre-t-il en partie le constat de la Sûreté de l'Etat suivant lequel, «le monde industriel se montre particulièrement circonspect dans ce genre d'affaires et ce, eu égard à son inquiétude vis-à-vis d'atteintes éventuelles à son image de marque ». Le Comité permanent R avait déjà signalé en ce qui le concerne : « l'importance du rôle d'un officier de sécurité dans une entreprise privée ainsi que la difficulté dans laquelle celui-ci peut se trouver d'avoir à déterminer la priorité parmi des intérêts privés et publics qui ne sont peut-être pas toujours concordants (voir rapport d'activités 2001 – p. 69 à 78).

4.5. En ce qui concerne la collaboration entre les différents services, le Comité permanent R constate que le SGRS a été quasi directement informé de la disparition inquiétante par le police fédérale. La Sûreté de l'Etat ne l'a été qu'un peu plus d'un mois plus tard à l'occasion d'une concertation bilatérale en matière d'enquêtes de sécurité avec le SGRS.

4.6. Le Comité permanent R relève qu'une fois informés de la disparition aussi bien la Sûreté de l'Etat que le SGRS ont collaboré avec les autorités judiciaires sur la base des dispositions d'une circulaire « confidentielle » du Collège des Procureurs généraux.

5. CONCLUSIONS ET RECOMMANDATIONS

5.1. Le présent dossier constitue un exemple concret supplémentaire relevé par le Comité permanent R sur l'indispensable nécessité d'assurer sur le plan de la sécurité un suivi effectif des entreprises présentant un intérêt stratégique.

5.2. Le Comité permanent R estime que, sur le plan de la transmission des premières informations en matière de sécurité, le délai de celle-ci devrait être amélioré aussi bien entre les officiers de sécurité des entreprises civiles et les services de renseignement, qu'entre les services officiels eux-mêmes.

En conclusion, d'un rapport précédent déjà cité ci-dessus, le Comité permanent R avait recommandé : « *la conclusion d'un accord spécifique entre les autorités judiciaires et les services de renseignement, dans le cadre de l'article 14 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Un tel accord devrait notamment viser à faciliter les échanges d'informations sur l'espionnage militaire, économique et scientifique entre ces autorités* ».

Dans un tel cadre, le Comité permanent R se demandait s'il ne convenait pas de réfléchir à l'élaboration d'une notice spécifique relative à l'espionnage économique, scientifique et industriel. Celle-ci s'ajouterait aux notices classiques du droit pénal commun. La notion de « vol » ne rend en effet pas compte de l'intention sous-jacente éventuelle d'espionnage ; elle ne permet pas non plus une exploitation statistique, analytique et criminalistique spécifique de ce phénomène au niveau national, voire international.
Le Comité permanent R réitère ces propositions.

5.3. Il recommande également de donner aux services de renseignement les moyens légaux, réglementaires techniques et humains nécessaires pour accomplir leur mission de sécurité des installations sensibles aux menaces définies dans la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Le Comité permanent R rappelle d'ailleurs que cette recommandation s'inscrit dans le contexte plus général de la problématique « de la défense du potentiel scientifique et économique du pays, ou de tout autre intérêt fondamental du pays défini par le Roi sur proposition du Comité ministériel du renseignement et de la sécurité » (cf. art. 7, 1° de la loi organique du 30 novembre 1998 précitée).

6. REACTIONS DES MINISTRES DE LA JUSTICE ET DE LA DEFENSE NATIONALE

Par courrier du 5 avril 2004, Madame le Ministre de la Justice a fait part au Comité permanent R de ce qui suit :

« *Si la Sûreté de l'Etat a collaboré avec les autorités judiciaires dans le cadre de ce dossier, je partage néanmoins les conclusions et les recommandations que le Comité R formule. Il me semble en effet important et urgent que l'on clarifie ce mode de collaboration entre les services secrets et les autorités judiciaires.*

Par ailleurs, en ce qui concerne la défense du potentiel scientifique et économique du pays ou de tout autre intérêt fondamental du pays défini par le Roi sur la proposition du Comité ministériel du Renseignement et de la Sécurité, je partage également la nécessité de recourir à une définition claire de ces concepts. Comme j'ai déjà pu vous l'indiquer, il entre dans mes intentions de mener une vaste réflexion sur le sujet et de la concrétiser par une décision au niveau du Comité interministériel du Renseignement et de la Sécurité ».

Par courrier du 13 avril 2004, le Ministre de la Défense nationale a communiqué au Comité permanent R l'avis suivant :

« Bien que le SGRS ait agi comme il devait après avoir été informé par la police fédérale le lendemain de la disparition, il y a certes encore des choses à améliorer dans le suivi des firmes titulaires d'une habilitation de sécurité sur le plan de la sécurité préventive. Je ne peux donc que souscrire à vos conclusions et recommandations.

Finalement, je n'ai pas d'objection à ce que ce rapport soit publié tel quel dans votre rapport annuel destiné au grand public ».

CHAPITRE 8: RAPPORT D'ENQUETE CONCERNANT LA GESTION D'UN INFORMATEUR PAR UN MEMBRE DE LA SURETE DE L'ETAT

1. FONDEMENT DE L'ENQUETE

Le Procureur du Roi de Termonde a adressé le 7 octobre 2002 au Comité permanent R une demande d'instaurer une enquête sur le comportement et les activités d'un membre de la Sûreté de l'Etat en relation avec un club sportif.

2. PROCEDURE

Etant donné qu'il s'agissait ici d'une enquête judiciaire, le Comité permanent R a initialement transmis cette mission pour exécution à son Service d'enquêtes, en application de l'article 40 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement. Après un échange de vues avec le Parquet de Termonde, le Comité permanent R, en réunion du 10 octobre 2002, a décidé dans la marge de l'enquête judiciaire, d'ouvrir une enquête de contrôle avec dénonciation éventuelle au Parquet de Termonde des faits délictueux qui seraient constatés.

Le présent rapport a été approuvé le 9 février 2004 par le Comité permanent R.

3. PORTEE ET CONTENU DE L'INFORMATION INITIALE

L'information initiale, relatée dans un procès-verbal du Service Judiciaire de l'arrondissement de Termonde relative à une enquête judiciaire globale à charge de la gestion d'un club sportif et l'asbl du même nom, mentionne :
"…*inlichtingen verkregen over mogelijke wanpraktijken in dienstverband door een lid van de Veiligheid van de Staat."*

4. DEVOIRS D'ENQUETE

Les devoirs suivants ont été menés afin d'évaluer les éléments cités ci-dessus et/ou de les placer dans un contexte plus concret :

- consultation du dossier judiciaire et le cas échéant, prise de copies utiles ,
- entretien avec les enquêteurs (service judiciaire de Alost) Termonde,
- demande en communication du dossier personnel
- demande en communication de l'enquête de sécurité

- consultation de toutes les données existantes à de la Sûreté de l'Etat
- entretien avec le Directeur des 'Opérations' de la Sûreté de l'Etat
- audition des chefs hiérarchiques
- audition des collaborateurs et des candidats à la succession de la personne concernée
- entretien avec les enquêteurs du « SCLC » (Service Central de lutte contre la corruption)
- audition du membre concerné de la Sûreté de l'Etat
- vérification des éléments complémentaires obtenus de sources diverses

5. CONCLUSION

L'objectif de l'enquête était de vérifier s'il y avait un rapport entre la fonction de comptable effectuée par l'intéressé auprès de la Sûreté de l'Etat et la gestion financière du club sportif.

L'enquête a montré qu'il n'y avait pas de relation avec les deux et qu'aucun élément suspect concernant la gestion financière par l'intéressé ne pouvait être retenu.

De l'enquête il ressort clairement que l'intéressé jouissait d'un régime de faveur. Il avait une grande liberté de mouvement et une grande flexibilité dans ses présences au service. L'origine de cette situation se situait dans les missions très confidentielles qui avaient été les siennes et également dans ses relations personnelles avec la hiérarchie dans le passé.

Ce dossier donne une image de la situation ancienne du service. De nouvelles techniques de « management » et l'arrivée en fin de carrière de l'ancienne génération (en ce compris l'intéressé) entraîne la disparition progressive de ces comportements du passé.

L'intérêt des constatations de l'enquête est d'avoir mis en évidence, au sein du service, l'existence de statuts personnels préférentiels qui ne peuvent plus se reproduire.

CHAPITRE 9 : ENQUETE DE CONTROLE CONCERNANT LA MANIERE DONT LA SURETE DE L'ETAT A TRAITE DES DOCUMENTS RECUS DU MINISTERE DES AFFAIRES ETRANGERES DANS LE CADRE D'UNE AFFAIRE DE VENTE D'ARMES FAISANT L'OBJET D'UNE ENQUETE JUDICIAIRE.

1. INTRODUCTION

Le Comité permanent R a appris que la Sûreté de l'Etat a été en possession de documents concernant une enquête judiciaire sur un trafic d'armes. Des questions ont été posées quant à la remise de ces documents. Il s'agissait de savoir si la Sûreté de l'Etat était bien le destinataire de ces documents et d'examiner de quelle manière ces documents avaient été traités.

2. ENQUETE

Le Service d'enquêtes a procédé à plusieurs interrogatoires du personnel concerné de la Sûreté de l'Etat et a recueilli des renseignements auprès du Ministère des Affaires étrangères et des autorités judiciaires.

Il ressort de ces enquêtes que la Sûreté de l'Etat était légitimement en la possession de ces documents et que l'objectif de l'expéditeur était précisément de remettre les documents à "tous les autres organismes officiels qu'ils pourraient intéresser".

L'enquête sur le traitement de ces documents a toutefois montré que la Sûreté de l'Etat avait eu une attitude hésitante quant à sa mission et à l'exercice de ses compétences propres concomitamment au déroulement d'une enquête judiciaire.
Comme cela a déjà été constaté dans d'autres dossiers, il semblerait que la Sûreté de l'Etat estime qu'une fois remis aux autorités judiciaires, les renseignements recueillis par le service dans le cadre de ses activités spécifiques revêtent un caractère strictement judiciaire et qu'elle ne peut plus agir de son propre chef.

Le Comité permanent R juge cette position injustifiée. Rien n'empêche la Sûreté de l'Etat de poursuivre l'exploitation des données recueillies dans le cadre de sa mission, même si celles-ci ont été portées à la connaissance des autorités judiciaires.

L'ouverture d'une enquête judiciaire n'est pas non plus une raison suffisante justifiant d'interrompre purement et simplement ses activités de renseignement.
Cela n'exclut pas pour autant de tenir compte de l'existence et des nécessités de l'enquête judiciaire. En pareil cas, une concertation avec les autorités judiciaires apparaît donc nécessaire.
Dans le présent dossier, cette concertation semble avoir eu lieu, après quelques hésitations, lors de la remise des documents aux autorités judiciaires.
Bien que cela ait été demandé au sein du service, aucune directive n'a été fournie de façon précise et impérative quant à la procédure à suivre.

3. CONCLUSION

Dans le présent dossier, aucune irrégularité n'a été constatée. Il ressort toutefois de l'enquête que la Sûreté de l'Etat a adopté une attitude hésitante, complètement injustifiée, à l'égard de ses propres compétences et qu'aucune directive ne lui a été donnée de manière précise et impérative.

CHAPITRE 10 : RAPPORT SUR LA MANIÈRE DONT LA SÛRETÉ DE L'ETAT A FONCTIONNÉ PAR RAPPORT À UNE INFORMATION ÉVENTUELLE DANS LE DOSSIER « FORD GENK » DANS LE CADRE DE SA MISSION DE PROTECTION DU POTENTIEL SCIENTIFIQUE ET ÉCONOMIQUE

1. INTRODUCTION ET PROCÉDURE

Au début du mois d'octobre, le Comité permanent R a été mis au courant par une personne désirant garder l'anonymat conformément à l'article 40 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement, de ce que la Sûreté de l'Etat aurait reçu, au début du mois de juin 2003, des informations concernant des mesures de licenciement de personnel de l'usine Ford à Genk.

Ces mêmes informations soulignaient également que la position de la Belgique pendant le conflit irakien aurait pu avoir une influence sur les décisions de la firme américaine.

Des informations provenant de sources ouvertes allant dans le même sens que ces supposées informations avaient déjà été publiées dans certains médias (cf. notamment un article du *« Trends »* du 19 juin 2003 et un article du *« Knack »* du 8 octobre 2003).

Dans des rapports précédents concernant la problématique de la défense du potentiel économique et scientifique de la Belgique dont la mission a été confiée à la Sûreté de l'Etat par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (cf. art 7,1°), le Comité permanent R avait déjà souligné en substance : que près de 5 ans après l'entrée en vigueur de la loi, aucune définition de ce potentiel n'a encore été donnée par le Comité ministériel du renseignement et de la sécurité, que la Sûreté de l'Etat n'a toujours pas les moyens nécessaires pour remplir cette mission, que nonobstant cette situation, ce service a entamé un travail de sensibilisation des secteurs tant privés que publics concernés, que des cas concrets ont été traités par la Sûreté de l'Etat.

Sur la base de ces éléments, le Comité permanent R a décidé lors de sa réunion du 9 octobre 2003 d'ouvrir d'initiative *« une enquête de contrôle sur la manière dont la Sûreté de l'Etat a fonctionné par rapport à une information éventuelle dans le dossier Ford Genk, dans le cadre de sa mission de protection du potentiel scientifique et économique. »*

Par courrier du 9 octobre 2003, Monsieur le Président du Sénat a été averti de l'ouverture de cette enquête, en application de l'article 32 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement.

La ministre de la Justice a été informée du début de l'enquête par lettre du chef du Service d'enquêtes du Comité permanent R le 9 octobre 2003, conformément au prescrit de l'article 43.1 de la loi organique précitée.

Suite à la demande de Madame la vice-première ministre et ministre de la justice (cf. les articles 33 et 35,3° de la loi du 18 juillet 1991 organique du Contrôle des services de police et de renseignement), le Comité permanent R s'est rendu le vendredi 9 octobre 2003 au siège de la Sûreté de l'Etat pour vérifier si effectivement ce service avait reçu au début du mois de juin 2003, les informations susdites et, le cas échéant, comment il les avait traitées et éventuellement communiquées aux autorités responsables.

Le jour même, vers 14 h, un rapport classifié «CONFIDENTIEL» au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité, a été transmis en deux exemplaires destinés respectivement à Madame la ministre de la Justice et à Monsieur le Premier ministre.

Le présent rapport portant la mention «DIFFUSION RESTREINTE» a été approuvé par le Comité permanent R lors de sa réunion du lundi 3 novembre 2003.

Il a été transmis à Madame la Ministre de la Justice le 5 novembre 2003 pour avis conformément à l'article 37 de la loi organique du contrôle des services de police et de renseignements.

2. INCIDENT PRÉALABLE À L'ENQUÊTE

Le jeudi 9 octobre 2003, le Comité permanent R était invité à présenter son Rapport général d'activités 2002 devant les Commissions parlementaires de suivi des Comités P et R, en application des articles 35 et 66 bis de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

L'article 35 prévoit notamment que : *"le Comité permanent R fait rapport à la Chambre des représentants et au Sénat annuellement, par un rapport général d'activités qui comprend, s'il échet, des conclusions et des propositions d'ordre général et qui couvre la période allant du 1er janvier au 31 décembre de l'année précédente. »*

L'article 66 bis indique dans son §3 que : *«les commissions siègent ensemble pour : examiner les rapports annuels des comités permanents avant leur publication…. »*

Le même article dans son § 5 prévoit que : *« **Les membres des commissions** prennent les mesures nécessaires afin de garantir le caractère confidentiel des faits ou renseignements dont ils ont eu connaissance en raison de leurs fonctions et sont soumis à une obligation de confidentialité. Ils sont dépositaires des secrets qui leur sont confiés dans l'exercice de leur mandat et même lorsqu'ils ont cessé leurs fonctions. Toute violation de cette obligation de confidentialité et de ce secret sera sanctionnée conformément au règlement de la Chambre à laquelle ils appartiennent. »*

Les membres du Comité permanent R sont quant à eux tenus à un secret professionnel sanctionné pénalement (cf article 64 de la loi organique précitée) ainsi qu'au respect des dispositions légales en matière de classification et d'habilitations de sécurité.

Le Comité permanent R sur ces bases et préalablement à la réunion susdite du 9 octobre 2003 avait décidé d'informer les deux Commissions de l'ouverture de la présente enquête.

Cette décision était motivée par le fait que dans le Rapport général d'activités 2002, le Comité permanent R faisait état des résultats d'une *« enquête complémentaire sur la manière dont la Sûreté de l'Etat s'acquitte de sa nouvelle mission de protection du potentiel scientifique ou économique ».*

En conclusion de ce nouveau rapport, le Comité permanent R recommandait une fois de plus de définir le potentiel scientifique et économique. A ce propos, tout en se montrant conscient de la difficulté de définir une telle mission, le Comité permanent R estimait toutefois qu'il y avait urgence à le faire pour permettre à la Sûreté de l'Etat de s'impliquer plus avant et de manière plus active dans ce domaine particulièrement d'actualité.
Dans la foulée, le Comité permanent R revenait aussi sur une ancienne recommandation de donner à la Sûreté de l'Etat les moyens légaux, techniques et humains appropriés pour exercer cette mission.

Le rapport général d'activités 2002 faisait encore référence à deux autres cas concrets que le Comité permanent R trouvait exemplatifs en matière de défense du potentiel scientifique et économique, à savoir : le *« Rapport de l'enquête de contrôle sur les éventuelles activités de la Sûreté de l'Etat concernant la protection du potentiel économique et scientifique lors de la faillite de la firme KPNQwest »* et le « R*apport sur l'intérêt qu'ont porté les services de renseignements à un vol de données sensibles commis dans une société commerciale belge fournissant des produits et services de hautes technologies. »*

Le Comité permanent R a donc estimé que dans le contexte ainsi rappelé, l'information donnée aux deux commissions parlementaires de suivi réunies à huis clos, de l'ouverture de la présente enquête constituait une indication légitime sur la façon de suivre concrètement l'évolution du travail de la Sûreté de l'Etat en cette matière.

A l'issue de cette réunion à huis clos, les informations qui devaient faire l'objet de l'enquête ont été portées à la connaissance de plusieurs médias en violation des dispositions légales reprises ci-dessus. C'est ainsi que l'expression d'une question soumise à vérification dans le cadre d'une enquête légale de contrôle, s'est transformée faussement en affirmation dépourvue de toute nuance et de toute pertinence.

Ces communications ont donné lieu à des incidents et à des interpellations politiques, ce qui a justifié la demande verbale du 9 octobre 2003 de Madame la Vice-première ministre et ministre de la justice qui priait le Comité permanent R d'effectuer d'urgence les vérifications à la Sûreté de l'Etat et d'en dresser rapport à son attention et à celle du Premier ministre le même jour avant midi (cf point 1 ci-dessus).

3. LES RÉSULTATS DES VÉRIFICATIONS À LA SÛRETÉ DE L'ÉTAT

Comme cela a déjà été mentionné ci-dessus, un rapport classifié « confidentiel » a été transmis aux ministres concernés. Ce document devait permettre à Monsieur le Premier ministre de répondre aux diverses interpellations du samedi 11 octobre 2003 devant les Commissions réunies de l'économie, de la politique scientifique, de l'éducation, des institutions scientifiques et culturelles nationales, des classes moyennes et de l'agriculture et des affaires sociales (voir Documents parlementaires – Com 023, Chambre 1ère session de la 51 E - législature 2003/2004, p 1 à 23).

Dans le cadre du présent rapport, le Comité permanent R ne peut donc que rappeler que selon ses constatations, les services extérieurs de la Sûreté de l'Etat avaient bien reçu au début du mois de juin 2003, de sources protégées par l'anonymat, les informations sensibles ; que celles-ci avaient fait l'objet d'une communication verbale de l'administrateur général « aux autorités » non autrement définies; que postérieurement à cette communication aucune autre démarche ou analyse visant à évaluer la valeur de ces informations n'avait été entreprise par ce service de renseignement.

4. CONSTATATIONS ET CONCLUSIONS

La nouvelle mission de défense du potentiel économique et scientifique pose incontestablement des problèmes de définition et de délimitation concrètes non seulement à la Sûreté de l'Etat, mais également aux responsables politiques.

Ces problèmes se doublent en ce qui concerne la Sûreté de l'Etat d'une difficulté à définir et à appliquer de manière rigoureuse une stratégie du renseignement principalement en ce qui concerne le traitement et l'analyse de l'information.

La communication en temps opportun de renseignements stratégiques pertinents reste un domaine où des efforts incontestables doivent porter.

Enfin, le Comité permanent R demande également qu'une réflexion ait lieu concernant les problèmes posés dans la pratique par les difficultés de respect de la confidentialité. Celle-ci représente en effet l'élément central qui garantit un contrôle démocratique et efficace des services de renseignement. Sans cette clé de voûte, le contrôle ne peut être que discrédité et se transformer en un contrôle alibi.

5. REACTION DE MADAME LA MINISTRE DE LA JUSTICE

Par courrier du 22 décembre 2003, Madame la Ministre de la Justice à communiqué son avis concernant le rapport. Cet avis mentionne, en substance, que la ministre de la Justice partage pour l'essentiel les constatations du Comité permanent R .

CHAPITRE 11 : RAPPORT DE L'ENQUETE DE CONTROLE SUR « LA MANIERE DONT LES SERVICES DE RENSEIGNEMENTS BELGES ONT SUIVI LES ACTIVITES D'UN REFUGIE PALESTINIEN EN RELATION AVEC DES GROUPES EXTREMISTES, TERRORISTES OU CRIMINELS ORGANISES.

1. INTRODUCTION

Au mois de décembre 2003, la presse a abondamment relaté l'interpellation et l'arrestation d'un certain Khalil Muhammad Abdallâh Al-Nawawreh, réfugié palestinien, par les services de police. Cette interpellation eut lieu dans le cadre d'une enquête judiciaire diligentée par le parquet d'Oudenaarde à la suite de braquages de bureaux de poste à Brakel, en décembre 2002, et à Court Saint Etienne, en février 2003.

Selon la presse, cet individu est suspecté d'avoir participé à des braquages à l'aide d'explosifs alors que son séjour en Belgique était soumis à des conditions assez strictes de résidence. Il ne séjournerait plus dans la résidence qui lui avait été assignée depuis le mois de juin 2002. Il aurait entretenu des contacts avec des personnes ayant elles-mêmes des liens avec des milieux criminels, islamistes et terroristes à Bruxelles.

Khalil Muhammad Abdallâh Al-Nawawreh est membre des milices «Tanzim », branche armée du Fatah, parti du Président de l'autorité palestinienne Yasser Arafat. Al-Nawawreh fut l'un des treize Palestiniens « bannis » par Israël, en mai 2002, à l'issue de la levée par l'armée israélienne du siège de 29 jours de l'église de la Nativité où s'étaient retranchés une centaine de Palestiniens.

A l'époque, dans le souci de permettre un dénouement non-violent de la situation et en accord avec l'Union européenne, la levée du siège de l'édifice religieux avait été négociée avec l'Etat d'Israël et acceptée moyennant l'exil de 13 de ses occupants.

Ceux-ci, après avoir transité par l'île de Chypre, ont trouvé refuge les uns en Italie, d'autres en Espagne, en Grèce, en Irlande et au Portugal.

Le 22 mai 2002, la Belgique accepta d'accueillir de manière temporaire, soit pour une durée d'un an, M. Khalil Muhammad Abdallâh Al Nawawreh avec le statut de réfugié pour raisons humanitaires. Le 19 octobre 2003, M. Al Nawawreh obtint une nouvelle autorisation de séjourner en Belgique pour une durée d'un an.

Compte tenu de l'intérêt manifesté par certains parlementaires pour cette affaire, le Comité permanent R a décidé le 18 décembre 2003 d'ouvrir une enquête de contrôle sur *«la manière dont les services de renseignements belges ont suivi les activités d'un réfugié palestinien en relation avec des groupes extrémistes, terroristes ou criminels organisés. »*

2. PROCEDURE

Par apostille du 18 décembre 2003, le Comité permanent R a chargé le Service d'enquêtes d'enquêter sur le suivi des activités de Khalil Muhammad Abdallâh Al Nawawreh depuis son arrivée en Belgique par les services de renseignement belges, de s'informer sur la coopération entre les différents services et d'obtenir les rapports éventuellement adressés aux autorités belges et/ou étrangères sur cette personne.

La ministre de la Justice et le ministre de la Défense Nationale en furent avertis le 22 décembre 2003.

Par retour du courrier Madame la Ministre de la Justice a pris acte de l'ouverture de cette enquête en attirant toutefois l'attention du Comité sur *«la circonstance que, dans le cadre de la convention qui a été conclue avec les autorités européennes, la Sûreté de l'Etat n'a, à aucun moment, été chargée d'une mission particulière de surveillance concernant ledit réfugié palestinien (...). La Sûreté de l'Etat n'avait donc aucune obligation de surveillance spécifique à exercer à l'égard de l'individu.»*

Le Service d'enquêtes R a procédé à des constatations durant les mois de janvier et de février 2004. Il a déposé son rapport le 27 février 2004.

Le présent rapport a été approuvé le 16 mars 2004.

3. L'INTÉRÊT PARLEMENTAIRE POUR LA QUESTION

Dès l'annonce de son arrivée en Belgique en mai 2002, de nombreux parlementaires ont interpellé le gouvernement afin d'exprimer leur intérêt ou leurs préoccupations à l'égard de la situation résultant de l'accueil de M. Khalil Muhammad Abdallâh Al-Nawawreh. C'est ainsi que le gouvernement a pu donner les explications suivantes.

L'arrivée de M. Khalil Muhammad Abdallâh Al-Nawawreh dans notre pays résulte de l'accord intervenu entre le gouvernement israélien et l'autorité palestinienne grâce à la médiation de l'Union européenne afin de permettre l'évacuation pacifique de l'église de la Nativité d'une part et le transfert ainsi que l'accueil de 13 occupants dans certains Etats membres de l'Union européenne d'autre part.

Le 22 mai 2002, la Belgique accepta d'accueillir de manière temporaire, soit pour une durée d'un an, M. Khalil Muhammad Abdallâh Al Nawawreh avec le statut de réfugié pour raisons humanitaires.

Après avoir précisé que les conditions d'accueil avaient été définies dans une position commune adoptée dans le cadre de la politique étrangère et de sécurité commune de l'Union européenne, le Ministre de l'Intérieur fit savoir que Khalil Muhammad Abdallâh Al-Nawawreh et l'Autorité palestinienne s'étaient engagés à respecter toutes les mesures de sécurité, actuelles et futures, imposées par la Belgique.

Tant que la sécurité l'exigerait, la Belgique déterminerait la résidence de Khalil Muhammad Abdallâh Al-Nawawreh dont les divers contacts requerraient par ailleurs une autorisation préalable de l'autorité compétente.

Le ministre de l'Intérieur ajouta que la délivrance d'un visa de séjour dans notre pays avait été subordonnée à l'acceptation, par Khalil Muhammad Abdallâh Al-Nawawreh, des conditions de sécurité visant sa propre protection et la sécurité publique en Belgique ainsi que dans les autres Etats membres de l'Union.

Le ministre précisa également que les conditions d'accueil pouvaient à tout moment être assouplies ou renforcées et que le Collège du Renseignement et de la Sécurité avait été chargé de suivre ce dossier.

Le Ministre des Affaires étrangères s'opposa pour sa part à divulguer le contenu des pourparlers ayant abouti à l'accueil en Belgique de M. Al Nawawreh dans le souci « *d'éviter des manœuvres de récupération démagogiques qui ne sont pas de nature à servir la paix au Proche-Orient ».*

L'arrestation de M. Al-Nawawreh en décembre 2003 fut l'occasion de nouvelles interpellations parlementaires auxquelles le gouvernement répondit de la manière suivante.

Le nouveau ministre de l'Intérieur déclara en substance que la présence en Belgique de Khalil Muhammad Abdallâh Al-Nawawreh découlait d'une décision de l'Union européenne d'accueillir dans les divers Etats membres les treize Palestiniens « bannis » impliqués dans l'occupation de la Basilique de la Nativité à Bethléem.

Partant, l'intéressé n'était donc pas demandeur d'asile et pouvait donc se déplacer librement sur notre territoire sans pouvoir être assigné à résidence. Le Ministre précisait également que suite à son arrestation, la Belgique devrait à nouveau aborder ce dossier avec l'Union européenne.

Pour le surplus, le ministre réfuta catégoriquement le qualificatif de « terroriste » attribué par certains à Khalil Muhammad Abdallâh Al-Nawawreh et il expliqua ne pas pouvoir revenir unilatéralement sur l'engagement de la Belgique vis-à-vis de l'Union européenne.

Sur le fond, le Ministre exposa que, dans un premier temps, l'intéressé avait scrupuleusement respecté ses obligations. La famille d'accueil avait régulièrement adressé des rapports au sujet de ses activités. Ce n'est que depuis le mois de mai 2003 qu'il respecta de moins en moins ses obligations, non sans être suivi en permanence. Toujours selon le Ministre, il fallait convaincre le Palestinien de revenir à Bertrix, par la concertation uniquement, sans possibilité de recours à la coercition.

Des parlementaires ont questionné le ministre de l'Intérieur sur les conditions d'accueil et de suivi du Palestinien « banni » tandis que d'autres l'on interrogé sur les liens que l'individu aurait établis des liens avec des milieux terroristes et islamistes. L'un d'eux demanda si la Sûreté de l'Etat ou un autre service avait informé le Ministre de l'Intérieur du fait que Khalil Muhammad Abdallâh Al-Nawawreh s'était écarté des conditions qui lui avaient été imposées durant son séjour en Belgique.

Le ministre répondit qu'il recevait des informations de la Police Fédérale et locale, de l'Office des Etrangers ainsi que du ministère des Affaires Etrangères et que ces informations étaient à la disposition des membres du Parlement.

4. LES INFORMATIONS PARUES DANS LA PRESSE AU SUJET DE M. KHALIL MUHAMMAD ABDALLÂH AL-NAWAWREH.

A son arrivée en Belgique, plusieurs quotidiens belges[181] ont décrit M. Khalil Muhammad Abdallâh Al-Nawawreh comme étant « *l'un des moins dangereux* » des treize « bannis » par Israël. Né en 1978, il est présenté comme membre de la milice « Tanzin Fatah », branche armée du parti du Président de l'autorité palestinienne Yasser Arafat.

Serge Dumont, correspondant du quotidien *« Le Soir »* en Israël, relevait toutefois que, selon la Sûreté générale israélienne et le service de renseignement militaire, l'intéressé aurait été l'un des adjoints du chef de la milice Tanzim et des brigades des martyrs d'Al Aksa de sa région. Il aurait ouvert le feu à de nombreuses reprises sur des appartements d'une colonie juive de Jérusalem et il serait également soupçonné d'avoir été mêlé à l'assassinat d'un civil israélien.

En août 2002, un journal francophone publia une interview de Khalil Muhammad Abdallâh Al-Nawawreh[182]. Un parlementaire fit remarquer il s'agissait d'une entorse à l'une des conditions émises pour l'accueil de ce Palestinien qui interdisait tout contact avec la presse[183].

Cet article révèle que Khalil Muhammad Abdallâh Al-Nawawreh vit dans une famille de réfugiés palestiniens dans un village wallon. Son « tuteur » qui l'héberge doit fournir un rapport quotidien de ses activités aux autorités belges. Les mesures de surveillance du début et les visites quotidiennes de la police se sont relâchées. Il a la nostalgie de son pays. Sa famille, à laquelle il téléphone tous les jours, et sa terre lui manquent plus que tout.

L'article relate également qu'il semble établi que Khalil Muhammad Abdallâh Al-Nawawreh « *ne correspond pas tout à fait au profil dressé par Israël »*, qu'il se tient parfaitement tranquille en respectant à la lettre les conditions de séjour imposées en Belgique au point de ne présenter aucun intérêt pour la police fédérale, et *«qu'il se murmure même, que la Sûreté belge aurait démonté la plupart des accusations que l'Etat hébreu avait inscrites dans son dossier. »*

La presse s'est également intéressée à la milice Tanzim à laquelle appartient M. Al Nawawreh. En résumé, le Tanzim est la branche armée du Fatah, parti du Président de l'Autorité palestinienne, créé en 1995, dans le but notamment de contrer le développement des groupes palestiniens islamistes radicaux.

Fidèle à Arafat ce groupement lui sert de milice officieuse et lui permet d'agir officieusement contre les intérêts israéliens, sans risquer une condamnation internationale pour violation des accords de paix. Sa structure d'organisation est fondée sur une division en secteurs géographiques, eux-mêmes subdivisés en cellules.

Le Tanzim, qui prétend compter des milliers de membres, dont la majorité sont des adultes palestiniens âgés de 20 ans à 35 ans, « diplômés de l'Intifada », résidant dans les territoires autonomes palestiniens, est présent dans chaque village et dans chaque camp de réfugiés.

---

181 «Le Soir » et « La Libre Belgique » des 21, 22 et 24 mai 2002, ainsi qu'une dépêche de l'agence Belga du 23 mai 2003.

182 «*Dans son refuge, quelque part en Wallonie, Khalil Al-Nawawreh rêve de Palestine »* Le Soir 12 août 2002.

183 Chambre 2° session de la 51°Législature,2003-2004 , séance du 18/12/2003

Des membres du Tanzim sont constamment impliqués dans la majorité des attaques armées contre les véhicules israéliens dans la bande de Gaza.

5. LES RENSEIGNEMENTS RECUEILLIS, TRAITÉS ET COMMUNIQUÉS AUX AUTORITÉS PAR LA SÛRETÉ DE L'ÉTAT

Le Comité permanent R et son Service d'enquêtes ont pu prendre connaissance de plusieurs notes et rapports adressés aux autorités par la Sûreté de l'Etat concernant M. Al Nawawreh. La plupart de ces informations ont été classifiées « secret » ou « confidentiel », ce qui ne permet pas au Comité permanent R d'en donner connaissance dans le présent rapport.

La Sûreté de l'Etat a d'emblée fait valoir qu'elle n'avait pris aucune part dans la décision de nature politique d'accueillir M. Al Nawawreh en Belgique et qu'elle n'avait reçu aucune instruction de la part de ces autorités de suivre cette affaire ou de surveiller le réfugié.

Ceci n'a pas empêché la Sûreté de l'Etat, eu égard à ses missions légales, d'assurer un certain suivi de ce dossier et de communiquer son avis *«aux ministres qui le sollicitaient lors des réunions organisées par leurs soins et d'informer les ministres de l'Intérieur et des Affaires étrangères».*

La Sûreté de l'Etat a effectivement assisté régulièrement aux réunions consacrées à la présence de M. Khalil Muhammad Al-Nawawreh en Belgique. Au départ, ces réunions ont été tenues au sein du Collège du Renseignement et de la Sécurité. Par la suite, elles furent organisées sous l'autorité du Ministre de l'Intérieur.

Dès le départ, la Sûreté de l'Etat a fait savoir à l'ensemble des ministres et autorités concernées que, selon des informations obtenues d'un correspondant étranger, « *les 13 palestiniens expulsés vers Chypre ont tous un lourd passé terroriste* ». Et la Sûreté de l'Etat de mettre en garde : *« La Sûreté de l'Etat ne peut pas garantir que ces gens resteront inactifs sur le territoire belge, ni s'engager dans le contrôle des activités des intéressés ».*

Dans ce contexte, la Sûreté de l'Etat a exprimé plusieurs fois verbalement ses plus vives réserves quant aux problèmes de sécurité liés au séjour en Belgique de M. Al Nawawreh. Pendant son séjour en Belgique, la Sûreté de l'Etat n'a cependant décelé aucune trace d'activisme politique extrémiste ou terroriste de la part de M. Al Nawawreh.

Néanmoins, le 22 mai 2003, la Sûreté de l'Etat a fait savoir aux ministres de l'Intérieur et des Affaires étrangères, ainsi qu'à l'Office des étrangers qu'elle estimait inopportun de prolonger le permis de séjour M. Nawawreh en Belgique au-delà du premier terme fixé en 2002.

Le 14 octobre 2003, la Sûreté de l'Etat a informé les ministres de l'Intérieur et des Affaires Etrangères que M. Al Nawawreh ne respectait pas les conditions fixées par l'Office des étrangers à son accueil dans notre pays. Il n'était à cet égard toutefois pas question d'activités entrant dans la sphère de compétence de la Sûreté de l'Etat au sens de la loi du 30 novembre 1998, mais plutôt d'activités délictueuses de droit commun.

Le 28 octobre 2003, après que M. Nawawreh a obtenu la prolongation de son autorisation de séjour en Belgique, la Sûreté de l'Etat a, une nouvelle fois, averti les ministres de l'Intérieur et des Affaires étrangères que l'intéressé entretenait des contacts avec des personnes suspectes d'activités délictueuses : *«de kringen waarin Al Nawawreh zich de laatste tijd begeeft, mogelijkerwijs ook verder in de toekomst een vlekkeloos verblijf in ons land kunnen hypothekeren » (**traduction libre** : « le milieu que Al Nawawreh fréquente ces derniers temps est susceptible d'hypothéquer un séjour sans tache dans notre pays pour l'avenir »).*

A la même date, la Sûreté de l'Etat a fait savoir à la police locale du lieu de résidence de M. Al Nawawreh que malgré les « *dispositions négatives* » de l'intéressé, ce dernier ne menait pas, à sa connaissance, d'activités extrémistes sur le territoire belge.

Le 23 janvier 2004, à la demande de la ministre de la Justice, la Sûreté de l'Etat lui a adressé un rapport de synthèse sur toute l'affaire. Ce service fait valoir qu'il ne dispose toujours pas de preuve d'une quelconque implication d'Al Nawawreh dans des délits de droit commun.

6. LES RENSEIGNEMENTS RECUEILLIS, TRAITÉS ET COMMUNIQUÉS AUX AUTORITÉS PAR LE SGRS

Au SGRS également, les informations disponibles sur cette affaire sont classifiées et ne peuvent dont être rendues publiques.

Au printemps 2002, un responsable du SGRS a été invité à participer à plusieurs réunions de coordination au sein du Collège du Renseignement et de la Sécurité dans le cadre de l'arrivée en Belgique de Khalil Muhammad Al-Nawawreh. Le SGRS n'a cependant reçu aucune tâche spécifique dans le suivi de cette affaire.

Néanmoins, en mai 2002, le SGRS a manifesté la plus grande attention quant à l'accueil par la Belgique du Palestinien Khalil El Nawawreh. En juin 2002, la section Contre-Terrorisme a produit un rapport détaillé à son sujet.

Dans ce rapport, destiné à Monsieur le Ministre de la Défense, étaient analysées les activités et les liens de tous les groupes palestiniens, y compris du Tanzim - Fatah dont Nawawreh est membre. Le SGRS n'a pas suivi ses activités en Belgique dans la mesure où la mission principale de ce service se concentre sur les intérêts militaires.

Le SGRS a produit une étude dans laquelle il analyse la décision de l'Union européenne d'ajouter six organisations palestiniennes sur sa liste terroriste, parmi lesquelles figurent les « *Brigades des Martyrs d'Al Aqsa* **»** qui se composent des mêmes combattants du « *Tanzim-Fatha »*.

Le SGRS en a logiquement conclu que l'Union européenne qui avait accueilli huit membres du « *Tanzim – Fatah* », avait donné refuge à huit terroristes. Cette étude fut distribuée à l'OTAN, au SHAPE, à la Sûreté de l'Etat, ainsi qu'à plusieurs services de renseignements alliés.

Le SGRS a estimé que les risques quant à la sécurité de M. Nawawreh étaient faibles aussi longtemps que celui-ci ne quittait pas le territoire belge sans autorisation.

7. CONCLUSIONS

La Sûreté de l'Etat n'a pris aucune part dans la décision d'accueillir M. Khalil Muhammad Abdallâh Al-Nawawreh en Belgique mais elle a mis les autorités en garde à propos du passé réputé terroriste de l'intéressé, membre du Tanzin - Fatah.

Bien que n'étant chargé d'aucune mission spécifique à cet égard, la Sûreté de l'Etat a néanmoins suivi la situation résultant de l'accueil en Belgique de ce réfugié. La Sûreté de l'Etat a remarqué que l'intéressé ne respectait pas les conditions mises à son accueil en Belgique et a averti les ministres des Affaires étrangères et de l'Intérieur des contacts qu'il entretenait avec des personnes suspectées d'activités délictueuses.

La Sûreté de l'Etat n'en a toutefois averti la ministre de la Justice que le 23 janvier 2004, à sa demande. La Sûreté de l'Etat avait préalablement informé l'ensemble des autorités compétentes des risques de sécurité engendrés par cette situation tout en respectant les choix politiques du gouvernement et de l'Union européenne.

Le SGRS n'a pas suivi les activités de M. Khalil Muhammad Abdallâh Al-Nawawreh en Belgique puisque la présence de cette personne dans le pays ne représentait aucune menace pour la sécurité militaire. Le SGRS a néanmoins produit une analyse estimant que l'Union européenne avait accueilli des personnes appartenant à une organisation qu'elle avait elle-même placée sur la liste des organisations terroristes.

Le SGRS et la Sûreté de l'Etat ont échangé quelques informations sur cette affaire.

8. RÉACTION DE MADAME LA MINISTRE LA JUSTICE

Par courrier du 5 avril 2004, Madame la Ministre de la Justice a fait savoir au Comité permanent R qu'elle n'avait *"rien d'autre à ajouter par rapport aux conclusions reprises dans ledit rapport".*

C. PLAINTES DE PARTICULIERS ET DENONCIATION

CHAPITRE 1: RAPPORT SUR L'ENQUETE MENEE A LA SUITE D'UNE PLAINTE D'UN PARTICULIER RELATIVE A D'EVENTUELS CONTROLES DE SECURITE SUR SA PERSONNE

1. PROCEDURE

Le 7 juin 2001, M. « E », employé au service « Cargo » d'une compagnie aérienne, a adressé au Comité permanent R une lettre dans laquelle il faisait part de son étonnement à propos de la réponse négative, sans la moindre motivation, donnée par la BIAC (Brussels Airport Terminal Company) suite à sa demande d'obtenir un badge d'accès à l'aéroport de Zaventem. Il ne sait pas quelle est l'instance qui a examiné sa demande, ni pour quelle raison il a encouru un refus.

Le 22 juin 2001, le Comité permanent R a adressé une apostille au Service d'enquêtes, le priant d'entendre l'intéressé et si possible d'établir si un des services officiels de renseignements était concerné.

Cette audition a eu lieu le 3 juillet 2001 et le Comité permanent R en a été informé sans que cela n'apporte toutefois des données complémentaires utiles. Néanmoins, le Comité permanent R a décidé le 16 juillet 2001 d'ouvrir une enquête sur cette affaire.

Le ministre de la Justice et le président du Sénat en ont été informés et une nouvelle apostille a été adressée au Service d'enquêtes.

Le 26 octobre 2001, le Service d'enquêtes a fait rapport au Comité permanent R.

En raison d'autres priorités et après avoir pris connaissance de plaintes similaires, qui ont fait plus clairement ressortir que la procédure de demande « d'avis » à la Sûreté de l'Etat était appliquée dans une très large mesure, cette plainte a été réexaminée à la fin de 2002 et ensuite le dossier a été clôturé.

2. CONSTATATIONS

2.1. Audition du plaignant

Tel que cela ressort de la plainte de l'intéressé et de son audition, la situation peut être résumée comme suit :

Depuis de nombreuses années, il travaille dans le secteur du transport aérien pour différentes compagnies successives, dans plusieurs aéroports en Belgique et à l'étranger, notamment en Afrique.

A chaque reprise, il a reçu pour ses activités, les badges « nécessaires », c'est-à-dire les autorisations requises sous forme de carte d'accès pour accéder à des zones d'aéroports non autorisées au public, telles que le tarmac.

Peu après son engagement par une autre compagnie aérienne, il a été obligé, en même temps que tous les membres du personnel, d'introduire pour l'obtention d'un « badge » une demande à la BIAC, l'entreprise qui exploite l'aéroport de Zaventem.

Après avoir appris que l'octroi du badge lui avait été refusé sans la moindre motivation, il a pris contact avec le chef de la sécurité chez BIAC qui lui a répondu qu'il n'en connaissait pas non plus la raison.

Une deuxième demande a abouti au même résultat : le badge a été refusé sans motivation et il n'était toujours pas possible de savoir quelle instance avait pris cette décision et pour quelles raisons.

Le plaignant présume qu'une entreprise privée sous la direction d'un ex-général traite cette affaire. Chez BIAC, on lui aurait dit qu'il devait lui-même savoir ce qu'il avait fait.

Interrogé par le Service d'enquêtes du Comité permanent R à propos des raisons éventuelles de ce refus, le plaignant déclare n'en connaître aucune précise. En effet, son casier judiciaire est vierge. Il a cependant signalé que dans le passé, il a été au service de la firme de son beau-frère suspecté de faits punissables ; dans ce cadre, il a été à maintes reprises interrogé par la BSR mais sans plus.

2.2. Vérifications à la Sûreté de l'Etat

Comme demandé dans l'apostille au Service d'enquêtes, ce dernier service a vérifié dans quelle mesure la Sûreté de l'Etat était éventuellement concernée par cette affaire.

Cette question a reçu le 8 août 2001 une réponse immédiate de la part de la Sûreté de l'Etat confirmant que BIAC leur avait bien adressé une demande relative au plaignant.

Le Service d'enquêtes a également pu consulter la banque de données de la Sûreté de l'Etat et prendre connaissance d'informations classifiées concernant l'intéressé.

Dans deux cas, le plaignant est connu parce qu'il a travaillé pour des firmes ou des personnes suspectées ou « connues » dans le contexte de trafics illégaux. Dans un cas, l'information provenait du SGRS (service général de renseignement et de sécurité des forces armées).

Bien que le dossier ne contenait aucun fait établi, aucune preuve, aucune condamnation à charge du plaignant, la Sûreté de l'Etat a estimé, après examen, que les éléments en sa possession, devaient donner lieu à un avis négatif adressé à la BIAC.

Dans l'appréciation de la fiabilité d'une personne, il ne faut en effet pas uniquement tenir compte des faits connus mis à charge de l'intéressé lui-même, mais aussi de ses relations et de son environnement.

Cette dimension est d'ailleurs visée dans la législation sur les habilitations de sécurité comme par exemple dans le cas des personnes majeures cohabitant avec la personne pour qui l'habilitation est demandée et pour laquelle une enquête de sécurité est menée dans le cadre de la loi du 11 décembre 1998 (article 16, §4).

2.3. Procédure appliquée

Le Comité permanent R a pu, grâce à ce dossier, constater qu'à la demande de la BIAC, la Sûreté de l'Etat donne très souvent des avis sur des personnes travaillant à l'aéroport de Zaventem. D'après la Sûreté, elle serait ainsi interrogée quelque 10.000 fois par an. Sur ce nombre, 200 personnes en moyenne figurent dans leur propre documentation, ce qui n'entraîne toutefois que quelques 5 avis négatifs par an. Ces demandes de renseignements sont faites à l'initiative de la BIAC pour l'aéroport de Zaventem.

Une procédure similaire existe pour l'aéroport régional d'Oostende, mais n'était pas en vigueur au moment de l'enquête pour les autres aéroports régionaux. A signaler que la police est également interrogée.

Les demandes constituent donc une procédure standard appliquée quotidiennement qui, si aucune donnée n'est connue à propos de la personne en question, n'est pas archivée en tant que telle, du moins au moment de la présente enquête.

L'avis, lorsqu'il est négatif (ce qui semble être exceptionnel), n'est pas motivé ou étayé par des faits concrets à l'intention de la BIAC.

Cette entreprise n'est donc pas officiellement à même de motiver sa propre décision autrement qu'en se référant à l'avis négatif de la Sûreté de l'Etat. Dans le cas d'espèce aucune procédure, ni aucune motivation n'a été communiquée au requérant.

2.4. Questions juridiques à propos de la procédure appliquée

Soulignons tout d'abord la nécessité de procéder à un screening des personnes qui ont accès à des endroits non publics des aéroports ou qui sont dispensées de certains contrôles.

Bien avant les attentats du 11 septembre, il a malheureusement été constaté que l'aviation civile était hautement vulnérable à des risques tels que le terrorisme, l'immigration illégale, divers trafics illégaux et diverses formes de criminalité organisée (cf. plusieurs attaques spectaculaires sur les transports d'or et de diamant).

Les avis de sécurité donnés par la Sûreté de l'Etat (dans une enquête similaire entamée ultérieurement) sont, dans une lettre du 23 janvier 2003, juridiquement fondés par ce service sur les normes suivantes :

- l'article 6 du contrat de gestion du 14 août 1998 entre l'Etat belge et la BIAC ;
- les articles 6, 7, 8 et 9 de l'arrêté royal du 3 mai 1991 portant réglementation de la sûreté de l'aviation civile ;
- la directive du ministre de l'Intérieur du 10 février 1971 en vue de prendre des mesures préventives dans le cadre de la lutte contre la piraterie aérienne ;

- la décision du 29 juin 1973 du Comité national pour la sécurité de l'aviation civile (CNSA) ;
- la convention du 23 septembre 1971 telle qu'elle a été approuvée par la loi du 20 juillet 1976 visant la répression d'actes illicites dirigés contre la sécurité de l'aviation.

Ces textes peuvent être complétés par le « Règlement 2320/2002/eg » du Parlement européen et du Conseil fixant des règles communes en matière de protection de l'aviation civile ainsi que par la loi belge organique des services de renseignement et de sécurité du 30 novembre 1998.

Sur base de ces éléments, on peut conclure que la collecte de l'information, la conservation de données et également l'avis donné par la Sûreté de l'Etat à la BIAC répondent à une finalité légitime.

Cette légitimité doit cependant revêtir une forme concrète en tenant compte de tous les principes de bonne administration et de protection de la vie privée.

A remarquer toutefois que dans aucun des textes normatifs précités, il n'est dit explicitement que la Sûreté de l'Etat donne des avis à la BIAC. Dans ces textes, tout est exprimé en termes généraux édictant que l'Etat et les autorités compétentes doivent prendre toutes les mesures afin de garantir de manière optimale la sécurité de l'aviation civile.

La Sûreté de l'Etat mentionne dans les avis transmis à la BIAC que c'est à cette instance qu'il revient en dernier lieu de prendre la décision définitive et que l'avis de la Sûreté de l'Etat n'est qu'un des éléments de cette prise de décision. D'un point de vue formel, au moins, cette conception est correcte.

La question de savoir si le particulier qui court finalement le risque de se voir opposer un refus d'octroi d'un badge (avec toutes les conséquences que cela implique et qui peuvent aller jusqu'à un licenciement sec) bénéficie d'une protection suffisante de ses droits et de sa vie privée, est très pertinente, mais elle n'entre pas sensu stricto dans les compétences (ratione materiae) du Comité permanent R.

3. CONCLUSIONS ET RECOMMANDATIONS

Le Comité permanent R n'a constaté dans le dossier examiné aucune violation formelle des droits du plaignant par la Sûreté de l'Etat.

L'avis négatif de la Sûreté de l'Etat communiqué à la BIAC est basé sur des indications défavorables concordantes concernant l'environnement du plaignant.

La Sûreté de l'Etat dispose de la base légale et de la finalité pour transmettre cet avis à la BIAC. Cette base est constituée par la loi organique des services de renseignement et de sécurité du 30 novembre 1998 et par les diverses normes de protection de l'aviation civile.

Le Comité permanent R ne peut d'autre part que constater qu'il existe des potentialités légales pour effectuer les vérifications nécessaires tout en garantissant au citoyen le respect de ses droits.

Les avis donnés à la BIAC le sont en dehors du cadre des habilitations de sécurité telles quelles sont régies par la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité.

Le Comité permanent R n'a pas été informé pour le surplus d'une éventuelle décision du Comité ministériel qui aurait confié, dans ce domaine, à la Sûreté de l'Etat l'exécution d'enquêtes de sécurité. Cette possibilité prévue par l'article 7, 2° de la loi organique des services de renseignement et de sécurité.

A ce stade, le Comité permanent R estime donc que ces possibilités n'ont manifestement pas été utilisées.

Le Comité permanent R comprend très bien l'exigence d'un grand nombre de vérifications de sécurité qui doivent être effectuées dans des délais très courts et il peut donc admettre que les formalités de la procédure relatives aux habilitations de sécurité conformes aux termes de la loi de 1998 soient trop lourdes et trop lentes pour régler des cas semblables à celui de l'espèce.

Toutefois, et selon les déclarations de la Sûreté de l'Etat elle-même, seuls quelques centaines de dossiers posent chaque année des problèmes et une petite partie seulement aboutit en fin de compte à un avis négatif.

Pour ce genre de cas exceptionnels, il devrait être possible, en adaptant le cas échéant la législation sur les habilitations de sécurité, de développer une procédure rapide et efficace respectant les droits de l'intéressé et lui permettant de savoir à tout le moins quelle instance prend une décision et pour quels motifs. Cela lui permettrait éventuellement d'introduire un recours approprié.

Cela pourrait se faire d'une manière similaire à ce qui existe actuellement dans le cadre de la procédure en matière d'habilitations de sécurité qui prévoit un juste équilibre entre les droits de la société et les critères de sécurité d'une part et les droits du citoyen d'autre part.

Le Comité permanent R recommande donc de prévoir une procédure complémentaire à la procédure en matière d'habilitations de sécurité (loi du 11 décembre 1998) qui respecterait cet équilibre dans les cas où la Sûreté de l'Etat et le SGRS, après consultation de leurs fichiers, émettraient des avis négatifs sur des personnes.

Le Comité permanent R craint qu'en l'absence d'une telle réglementation, la responsabilité de l'Etat ne soit tôt ou tard mise en cause.

4. INFORMATION AU PLAIGNANT

En date du 2 avril 2003, le Comité permanent R a adressé un courrier au plaignant pour lui signaler que :

"*Conformément à la loi du 18 juillet 1991, les rapports d'enquête adressés aux autorités parlementaires et aux ministres compétents restent confidentiels et ne peuvent pas vous être transmis*

S'il n'est pas classifié, le rapport sera ultérieurement publié dans le rapport d'activités annuel du Comité permanent R. Le cas échéant, vous aurez, bien entendu, accès à cette version. Il va de soi que votre nom ne sera pas repris dans la version publiée.

Toutefois, sur base de l'article 66 du Règlement d'ordre intérieur du Comité permanent R, prévoyant le principe que le plaignant a le droit de connaître la suite qui a été réservée à sa plainte, je vous communique dès à présent ce qui suit.

La demande d'obtention d'un badge chez BIAC est soumise à une procédure administrative qui prévoit que BIAC soumet cette demande pour avis à la Police fédérale et à la Sûreté de l'Etat.

Le contenu du premier avis est inconnu du Comité permanent R. L'avis de la Sûreté de l'Etat était en tout cas négatif. Sur la base des dossiers concernés et de la législation existante, le Comité permanent R n'a pas constaté de violation par la Sûreté de l'Etat des droits du plaignant. L'avis est en effet fondé sur des indications concordantes.

Le Comité permanent R constate également que la Sûreté de l'Etat a agi légitimement en transmettant cet avis à BIAC. L'avis transmis ne contient aucune motivation.

La décision formelle de ne pas octroyer le badge a été prise par BIAC. Etant donné que le Comité permanent R est seulement compétent pour contrôler les services de renseignements belges, le Comité permanent R n'est pas qualifié pour porter un jugement sur la décision de BIAC.

Le Comité permanent R a recommandé de mettre en place une procédure légale qui autoriserait la réalisation d'enquêtes de sécurité ou de vérifications de sécurité. Cette future procédure devrait donner au plaignant le droit d'avoir connaissance de l'organe qui fait l'enquête, le droit de recevoir une décision motivée ainsi que le droit d'exercer un recours contre une décision négative éventuelle ».

CHAPITRE 2: RAPPORT D'ENQUETE RELATIF A LA PLAINTE D'UN PARTICULIER RELATIF AU COMPORTEMENT D'AGENTS DE LA SURETE DE L'ETAT

1. PROCEDURE

Le 1er avril 2002, le Comité permanent R a réceptionné la plainte d'un avocat dont le client mettait en cause des membres de la Sûreté de l'Etat.

Les éléments de la plainte peuvent être résumés comme suit :

En 1999, l'intéressé, d'origine étrangère, a obtenu le statut de réfugié politique en Belgique. Il collabora alors de manière épisodique avec la Sûreté de l'Etat.

Par la suite, cette collaboration se fit plus intense et l'intéressé devint un informateur rémunéré.

Dans le cadre de cette activité, il fera l'objet d'une plainte judiciaire de la part d'une personne avec laquelle il avait pris contact pour obtenir certaines informations. Il sera interpellé pour ces faits par la police.

Suite à cet incident, l'intéressé porta plainte auprès du Comité permanent P contre des agents de la police zonale. Il s'adressa également au Comité permanent R pour accuser la Sûreté de l'Etat de ne pas avoir respecté ses engagements financiers et d'avoir mis sa vie en danger.

Le 11 avril 2002, le Comité permanent R a ouvert une enquête de contrôle qui fut notifiée le 22 avril 2002 au Président du Sénat conformément au prescrit de l'art. 32 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

Le Ministre de la Justice a été averti par courrier du 22 avril 2002 de l'ouverture de l'enquête.

Le 3 décembre 2002, le Service d'enquêtes du Comité permanent R faisait part de ses constatations.

Le présent rapport a été approuvé lors de la réunion du 2 mars 2004 du Comité permanent R.

2. LES GRIEFS DU PLAIGNANT

Les griefs du plaignant à l'encontre de la Sûreté de l'Etat s'articulent selon deux axes.

En premier lieu, le plaignant affirme qu'une rencontre directe se serait déroulée entre un de ses contacts et des agents de la Sûreté de l'Etat. Cette rencontre directe aurait révélé son rôle d'informateur. Le contact aurait donc été perdu et le plaignant aurait par la suite reçu des menaces de mort.

En second lieu, le plaignant aurait été interpellé par la police sur plainte d'une personne qu'il avait approchée à la demande de la Sûreté de l'Etat en vue d'obtenir des informations. A cette occasion, il s'était fait passer pour un agent de l'Office des étrangers.

Ce dernier incident se trouve à l'origine de la décision de la Sûreté de l'Etat de mettre fin à sa collaboration avec l'informateur.

3. LES RESULTATS DE L'ENQUETE

Il ressort d'une manière générale des investigations menées par le Service d'enquêtes du Comité permanent R, qu'aucun élément ne permet de confirmer la version du plaignant quant aux reproches formulés à l'égard des agents de la Sûreté de l'Etat.

C'est ainsi que l'examen des documents relatifs aux rapports entre le plaignant et les agents de la Sûreté de l'Etat qui permettent de reconstituer partiellement les contacts de ceux-ci (devoirs effectués et frais engagés) ne révèle aucune anomalie, ni irrégularité.

D'autre part l'examen des rapports rédigés par les agents de la Sûreté de l'Etat reprenant les informations obtenues, exploitables et exploitées à l'intervention du plaignant confirme la collaboration de celui-ci dans le cadre de la problématique de la traite des êtres humains et de l'immigration illégale.

En ce qui concerne particulièrement le 1er grief, les déclarations des agents de la Sûreté de l'Etat contredisent de manière unanime les déclarations du plaignant. Pour ces agents, l'informateur n'aurait pas été opposé au contact direct des agents de la Sûreté de l'Etat avec une tierce personne en séjour illégal en Belgique, et cela dans le but de recueillir des renseignements sur l'immigration clandestine et le trafic d'êtres humains.

Le plaignant reconnaît d'ailleurs que bien qu'hostile à ce contact, il l'avait lui-même organisé.

Toujours selon les membres concernés de la Sûreté de l'Etat, la collaboration avec cette tierce personne n'aurait pas échoué à cause du dévoilement de la qualité d'informateur du plaignant, mais bien pour des raisons objectives et pratiques (exigences démesurées de la tierce personne contactée et problème linguistique lié à la méconnaissance de la langue de cette personne).

En ce qui concerne le second grief, les agents de la Sûreté de l'Etat réfutent la thèse soutenue par le plaignant selon laquelle il aurait tenté d'obtenir des informations en se faisant passer, à la demande de ces agents, pour un fonctionnaire de l'office des étrangers.

Les mêmes agents affirment qu'ils n'ont jamais donné la moindre instruction au plaignant quant à la manière de recueillir les informations qu'ils attendaient. Bien au contraire, selon eux, ils n'ont eu de cesse que de lui recommander la prudence dans les démarches d'investigations au sein de ce milieu criminel spécialisé dans le trafic d'êtres humains.

Toujours d'après eux, si le plaignant a usurpé une qualité de fonctionnaire dont il ne jouissait pas , ce fait procède uniquement d'une initiative qui lui est propre.
Ils déclarent de la même manière n'avoir donné, à l'occasion de l'interpellation du plaignant par les services de police, aucune précision sur la nature exacte des rapports que l'intéressé entretenait avec la Sûreté de l'Etat.

En tout état de cause, les auditions des agents de la Sûreté de l'Etat ainsi que les rapports d'information rédigés par ces agents ne contiennent aucun élément permettant de confirmer ou d'infirmer cette hypothèse.

Il est précisé à ce sujet que c'est le plaignant lui-même qui a téléphoné du poste de police à la Sûreté de l'Etat lors de son interpellation. Les services de police s'étaient en effet inquiété de la qualité de « membre de la Sûreté de l'Etat » invoquée par le plaignant au moment de leur intervention.

Le Comité permanent R note de surcroît que le volet policier de l'enquête de contrôle menée par le Comité permanent P a abouti à des conclusions similaires en ce qui concerne les griefs articulés par le plaignant à l'égard des policiers intervenant.

C'est ainsi qu'il ressort en conclusion de cette enquête du Comité P :

- Que le plaignant n'a pas été emmené manu militari par les services de police ;

- Que les policiers n'ont commis aucune violation du secret professionnel en dévoilant à des tierces personnes la qualité d'informateur de la Sûreté de l'Etat du plaignant ;

- Que le policier intervenant n'a pas refusé d'acter sa plainte.

4. CONCLUSIONS ET RECOMMANDATIONS

L'enquête de contrôle n'a pas mis en évidence les éléments qui indiqueraient que par leur comportement des membres de la Sûreté de l'Etat auraient porté directement ou indirectement atteinte à des droits et libertés garantis par la constitution et par la loi.

En l'espèce, rien n'indique que l'article 18 de la loi du 30 novembre 1998, organique des services de renseignement et de sécurité (« *Dans l'exercice de leurs missions, les services de renseignement et de sécurité peuvent avoir recours à des sources humaines. Dans ce cas, ces services doivent veiller à la sécurité des données qui concernent les sources humaines et des informations qu'elles communiquent* ») n'ait pas été respecté par les agents de la Sûreté de l'Etat.

Le présent cas d'espèce illustre, une nouvelle fois, les difficultés pratiques de l'utilisation d'informateurs[184] par les services de renseignements ainsi que l'impossibilité de retracer a posteriori les détails de la relation entre informateur et agent d'un service de renseignement. Il est d'autant plus difficile en cas d'incident, d'instruire les faits afin de mettre les éventuelles responsabilités en évidence.

Si le recours à des informateurs reste le moyen par excellence de recueillir de l'information, il n'existe toujours aucune règle précise pour encadrer l'utilisation de ce moyen humain dans le domaine du renseignement et la Sûreté de l'Etat s'est toujours montrée réticente à ce que cette matière soit réglementée par voie légale.

Des notes internes existent, mais dans la pratique, le Comité permanent R a maintes fois constaté, à l'occasion justement de cas litigieux, que la manière de traiter les informateurs semble laissée à l'appréciation ponctuelle des agents des services extérieurs.

Dans son rapport d'activités 2001 (p.193), si le Comité permanent R recommandait aux deux services de renseignement belges de ne pas négliger le recueil d'informations par des moyens humains (Humint), il recommandait également que le recours aux informateurs par ces services fasse l'objet d'un code de conduite et de directives claires relatives notamment à leur recrutement et à leur protection.

D'une manière générale, le Comité permanent R estimait aussi que l'utilisation de techniques spéciales de recherches intrusives pour la vie privée (écoutes, filatures, informateurs, infiltrations, …) par les services de renseignement devaient faire l'objet de normes légales prévoyant le respect des principes de subsidiarité et de proportionnalité. Le Comité permanent R estime qu'il y a urgence à régler ce problème, alors qu'une législation ad hoc existe pour les services de police. C'est d'ailleurs une nécessité de légiférer dans ce sens pour répondre aux normes internationales et constitutionnelles de protection de la vie privée des citoyens.

De telles dispositions, en matière de recueil du renseignement, sont indispensables aussi bien du point de vue de l'efficacité des services, que de celui de la protection des droits des citoyens et des fonctionnaires impliqués dans de telles activités.

Le Comité permanent R réitère ces recommandations.

[184] Dans son rapport d'activités 1997, le Comité permanent R proposait de cette notion, la définition suivante : "une personne qui, rémunérée ou non sollicitée ou spontanée, fournit des informations difficilement accessibles par d'autres voies et peut de ce fait encourir un risque matériel, moral ou physique".

CHAPITRE 3: RAPPORT D'UNE ENQUETE DE CONTROLE OUVERTE SUITE A LA PLAINTE D'UN CANDIDAT A LA NATIONALITE BELGE A L'EGARD DE L'AVIS FOURNI PAR LA SURETE DE L'ETAT SUR SA DEMANDE DE NATURALISATION

1. OBJET DE LA PLAINTE

Par courrier du 13 février 2003, un avocat a introduit au nom de son client une plainte auprès du Comité permanent R.

Au cours de l'année 2000, le plaignant a introduit une déclaration devant l'Echevin de l'Etat civil de sa commune selon laquelle il voulait obtenir la nationalité belge.

L'administration communale a transmis le même jour cette demande de naturalisation au parquet du tribunal de première instance, ainsi qu'à la Sûreté de l'État. Cet envoi a été réalisé en application de l'article 12bis du Code de la nationalité belge et de la circulaire du 25 avril 2000 relative à la loi du 1er mars 2000 modifiant certaines dispositions concernant la nationalité belge (Moniteur belge – 6 mai 2000).

L'avocat conteste les informations que la Sûreté de l'Etat a fournies au procureur du Roi, informations sur base desquelles ce dernier a formulé un avis négatif quant à la déclaration de nationalité du plaignant.

Cet avis négatif mentionne notamment que l'intéressé est connu de la Sûreté de l'Etat pour être un individu dangereux et armé, pour être membre d'une organisation politique étrangère extrémiste, pour être à l'origine de confrontations violentes avec des adversaires politiques et pour avoir renoncé à la nationalité belge qu'il possédait auparavant afin d'échapper au service militaire.

Le procureur du Roi estime que « *dans l'avis qu'il doit formuler dans la procédure de naturalisation, le ministère public doit déterminer sa position en tenant compte des informations que la Sûreté de l'Etat lui communique en application des missions que la loi attribue à ce service».*

Le plaignant conteste formellement les informations transmises au procureur du Roi par la Sûreté de l'Etat. Il admet avoir renoncé à sa nationalité belge afin de ne pas effectuer de service militaire en Belgique et il explique ce choix par les difficultés financières qu'il connaissait alors. Il regrette ce mauvais choix.

Il conteste par ailleurs appartenir à la tendance politique que la Sûreté de l'Etat lui attribue ; en Belgique, il voterait même pour un parti de tendance opposée. Il affirme ne pas s'intéresser aux affaires politiques de son pays d'origine et n'entretenir aucun lien avec quelque organisation politique étrangère que ce soit.
Il adhère aux valeurs démocratiques de notre pays et il n'est jamais armé. Il évoque une confusion possible entre lui et un parent homonyme qui, lui, serait un militant extrémiste.

L'avocat demande au Comité permanent R de mener une enquête sur la source des informations transmises au procureur du Roi.

2. PROCÉDURE

Le 20 février 2003, le Comité permanent R a décidé d'ouvrir une enquête concernant la Sûreté de l'Etat suite à la *plainte d'un particulier dans le cadre d'une procédure d'option de nationalité.*

Cette enquête porte aussi bien sur l'atteinte éventuelle que la Sûreté de l'Etat pourrait avoir causée aux droits du plaignant que sur l'efficacité de ce service.

Le Président du Sénat et la ministre de la Justice furent avertis du début de l'enquête par courrier du 21 février 2003.

L'avocat du plaignant a été informé de l'ouverture de cette enquête le 12 septembre 2003.

Le même jour une apostille a été adressée au Service d'enquêtes du Comité permanent R afin de se faire communiquer, en copie, le dossier de la Sûreté de l'Etat.

Le Service d'enquêtes et le Comité permanent R ont pris connaissance des rapports mentionnant le nom du plaignant à la Sûreté de l'Etat.

Une enquête complémentaire a été prescrite par le Comité permanent R le 10 septembre 2003 afin d'examiner plus avant l'hypothèse d'une confusion entre deux personnes homonymes.

Le présent rapport a été approuvé le 8 mars 2004.

3. LES INFORMATIONS DONT LA SÛRETÉ DE L'ETAT DISPOSE CONCERNANT LE PLAIGNANT

Le Comité permanent R a été mis en possession des rapports internes qui mentionnent le nom du plaignant, ainsi que des notes transmises au Procureur du Roi à l'occasion de sa demande de nationalité belge.

Le plaignant n'a jamais fait l'objet d'une enquête spécifique sur sa personne de la part de la Sûreté de l'Etat, ni au moment où ce service a reçu la notification de sa demande de nationalité belge, ni d'ailleurs auparavant.

Les renseignements communiqués au parquet ont été recueillis à l'occasion d'enquêtes générales menées sur des groupes politiques réputés extrémistes et actifs au sein d'une communauté allochtone établie dans une grande ville du pays.

Les notes communiquées au procureur du Roi n'indiquent pas quelle est la source ou quelles sont les sources qui sont à la base des informations qui lui sont communiquées (« *selon nos informations* »). La source est qualifiée de « fiable ». La protection des sources justifie ainsi la classification « secret » donnée aux rapports internes consultés.

Il n'apparaît pas du dossier consulté que les informations relatives au plaignant ont été recoupées par d'autres sources ni mises en rapport avec d'autres sujets traités par la Sûreté de l'Etat ou tout simplement actualisées avant d'être transmises au Procureur du Roi.

C'est probablement la raison pour laquelle la Sûreté de l'Etat a communiqué certaines informations au mode conditionnel (« *il aurait sciemment provoqué des troubles …* »). Ces informations mentionnent effectivement les faits et les comportements décrits plus haut et qui sont attribués au plaignant.

L'hypothèse d'une confusion avec un parent homonyme extrémiste a aussi été examinée plus avant et a fait l'objet d'un rapport séparé du Service d'enquêtes. Il en résulte qu'aucune confusion ne s'est produite entre le plaignant et une autre personne homonyme dans les informations que la Sûreté de l'Etat a communiquées au procureur du Roi.

Une vérification complémentaire a néanmoins fait apparaître une confusion auprès de l'Office des étrangers, imputable à la Sûreté de l'Etat. Cette confusion n'a eu aucune incidence sur l'avis formulé par le procureur du Roi.

Par ailleurs, le Comité permanent R ne peut que prendre acte des dénégations et des explications fournies par l'avocat du plaignant sans possibilité, pour sa part, de vérifier l'éventuelle appartenance ou non de ce dernier à un mouvement réputé extrémiste ni son prétendu rôle dans le déclenchement d'incidents violents avec des adversaires politiques.

Le Comité note cependant que l'information dont la Sûreté de l'Etat était en possession selon laquelle le plaignant aurait renoncé à sa nationalité belge afin d'échapper au service militaire le concerne bien et que son avocat le confirme. Ce rapport annonçait d'ailleurs que l'intéressé redemanderait sa nationalité belge dès lors qu'il serait sûr de ne plus être appelé sous les armes. Voici donc, au moins, une information qui se vérifie et qui est obtenue à la meilleure source possible.

4. CONCLUSIONS

Le Comité permanent R se pose la question de savoir s'il est justifié – lorsque l'on invoque un avis qui doit fonder une décision d'octroi ou de refus de la nationalité belge - que les autorités compétentes prennent une décision sur la base d'éléments conditionnels qui, comme cela apparaît dans le cas du plaignant, jouent en défaveur du requérant.

Les délais imposés par le législateur sont tels qu'ils ne permettent effectivement pas à la Sûreté de l'Etat, pour des raisons de manque de temps et de personnel, de traiter des dizaines de milliers de dossiers de naturalisation en y mettant le soin nécessaire.

Le fait que le service (qui est tenu de respecter des délais et qui transmet sont avis à des autorités qui, elles-mêmes, disposent de peu de temps pour évaluer les cas) ne peut analyser les éléments utilisés, a pour conséquence que tous les demandeurs ne disposent peut-être pas des même chances.

Là où certains vont sans doute pouvoir bénéficier de la procédure rapide d'acquisition de la nationalité belge en l'absence de vérification de leurs antécédents vu la pression des délais, d'autres par contre pourront se voir tout aussi rapidement refuser cette nationalité sur base d'éléments insuffisamment contrôlés.

Le cas du plaignant semble, en effet, ne pas être un cas isolé. Le Comité permanent R a en effet constaté dans d'autres dossiers de même nature, que la manière dont la Sûreté de l'Etat délivrait des avis sur des personnes à certaines autorités posait quelques problèmes. Le nœud de cette problématique est de savoir :

- De quelle manière et auprès de quelles instances des plaintes relatives à d'éventuelles violations de droits pourront être traitées ;

- De quelle manière les droits garantis par la Constitution et par les conventions européennes peuvent le mieux être respectés ;

- Comment rendre compatible la confidentialité nécessaire de certaines données avec l'obligation de donner connaissance à la partie lésée des éléments nécessaires à l'exercice de son action en réparation.

Le Comité permanent R a mené une étude sur ce sujet destinée aux ministres compétents et à sa commission parlementaire de suivi.

5. RÉACTION DE MADAME LA MINISTRE DE LA JUSTICE

Par courrier du 5 avril 2004, Madame la Ministre de la Justice a réagi de la manière suivante au rapport d'enquêtes :

« *Comme vous le soulignez à juste titre, « les délais imposés par le législateur sont tels qu'ils ne permettent effectivement pas à la Sûreté de l'Etat , pour des raisons de manque de temps et de personnel, de traiter des dizaines de milliers de dossier de naturalisation en y mettant le soin nécessaire ».*
Par ailleurs, je me permets d'insister sur la circonstance que la Sûreté de l'Etat fournit des avis à l'autorité judiciaire à qui incombe la responsabilité de remettre un avis final sur la demande de naturalisation.

Comme vous le savez, j'ai l'intention de déposer rapidement un avant-projet de loi relatif aux vérifications de sécurité opérées par la Sûreté de l'Etat . Il s'agira également d'aborder le problème des avis qu'elle fournit dans le cadre des demandes d'acquisition de la nationalité belge. Je suis donc extrêmement attentive à cette problématique ».

CHAPITRE 4: RAPPORT DE L'ENQUETE DE CONTROLE CONCERNANT LA PLAINTE D'UNE CANDIDATE A LA NATURALISATION A L'EGARD DE L'AVIS FOURNI PAR LA SURETE DE L'ETAT SUR SA DEMANDE DE NATURALISATION

1. OBJET DE LA PLAINTE

Par courrier du 27 mars 2003, un avocat a introduit au nom de sa cliente, Madame X, de nationalité étrangère, une plainte auprès du Comité permanent R.

Au cours de l'année 2002, la plaignante a introduit une déclaration devant l'Échevin de l'État civil de sa commune selon laquelle elle voulait obtenir la nationalité belge de son époux, conformément à l'article 16 du Code de la nationalité belge.

Le dossier contenant la demande d'obtention de la nationalité belge a été transmis le même jour par le fonctionnaire de l'État civil à la Sûreté de l'État. Cet envoi a été réalisé en application de l'article 12bis du Code de la nationalité belge et de la circulaire du 25 avril 2000 relative à la loi du 1er mars 2000 modifiant certaines dispositions concernant la nationalité belge (Moniteur belge - 6 mai 2000).

Par cette plainte, Madame X conteste les informations que la Sûreté de l'État a fournies au procureur du Roi, informations sur base desquelles ce dernier a formulé en novembre 2002 un avis négatif quant à la déclaration de nationalité de la plaignante.

Cet avis négatif mentionne notamment ce qui suit : *« Attendu que Madame X est connue de la Sûreté de l'État qui constate que l'intéressée serait membre de* (NDR : une organisation considérée comme extrémiste). *(…) Dans l'avis qu'il doit formuler dans la procédure de naturalisation, le ministère public doit déterminer sa position en tenant compte des informations que la Sûreté de l'État lui communique en application des missions que la loi attribue à ce service».*

Madame X conteste formellement les informations contenues dans ce rapport, en particulier en ce qui concerne son appartenance à un mouvement considéré comme extrémiste : *«Je dois donc contester formellement le contenu de ce rapport très sommaire – aucun détail n'est contrôlable - et vous demander d'exécuter une enquête à ce sujet».*

2. PROCÉDURE

Le 6 mai 2003, le Comité permanent R a décidé d'ouvrir une enquête concernant la Sûreté de l'État suite à la *« plainte d'un particulier dans le cadre d'une procédure d'option de nationalité ».*

Cette enquête porte aussi bien sur l'atteinte éventuelle que la Sûreté de l'État pourrait avoir causée aux droits de la plaignante que sur l'efficacité de ce service.

L'avocat de la plaignante a été informé de l'ouverture de cette enquête le 7 mai 2003.

Le même jour une apostille a été adressée au Service d'enquêtes du Comité permanent R afin de se faire communiquer, en copie, le dossier de la Sûreté de l'État.

Le Président du Sénat et la ministre de la Justice furent avertis du début de l'enquête par courrier du 8 mai 2003.

Le Service d'enquêtes et le Comité permanent R ont pris connaissance du dossier de l'intéressée à la Sûreté de l'État.

Le rapport de cette enquête a été adressé au ministre de la Justice et au président du Sénat le 23 décembre 2003.

A la même date, l'avocat de la plaignante a été informé des conclusions de ce rapport.

A la date du 29 février 2004, le Comité permanent R n'avait pas reçu l'avis du ministre compétent concernant cette affaire.

En application de l'article 37 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement, le Comité permanent R a décidé de rendre le présent rapport public en partie.

Ce document a donc été approuvé le 3 mars 2004.

3. CONSTATATIONS

Les renseignements que la Sûreté de l'Etat a transmis au Procureur du Roi concernant Madame X ont été recueillis il y a plusieurs années à l'occasion d'une enquête générale menée sur des partis extrémistes actifs au sein d'une communauté d'origine étrangère établie dans une grande ville. Il n'apparaît nulle part du dossier de la Sûreté de l'Etat que les données ainsi transmises ont été vérifiées et actualisées en réalisant une enquête sur l'intéressée.

Le renseignement communiqué au procureur du Roi provient d'une source à laquelle la Sûreté de l'Etat attribue un haut degré de fiabilité. Il s'agit donc d'une information collectée dans le cadre d'un travail de recueil de renseignements auprès d'informateurs et non d'une preuve qui aurait été recueillie dans le cadre d'une enquête judiciaire.

Dans le contexte d'une procédure de naturalisation, le Comité permanent R estime que cette information n'était pas suffisamment contrôlée pour pouvoir objectivement et de manière pertinente affirmer que Madame X serait membre d'un groupement décrit comme fondamentaliste. De plus, du fait qu'il n'y a eu aucune actualisation, le service ne dispose d'aucun élément qui confirme qu'elle en est encore membre et partant qu'elle jouerait un rôle actif de cette association considérée comme potentiellement dangereuse.

Par ailleurs, le Comité permanent R ne peut donc que prendre acte des dénégations et des explications fournies par l'avocat de la plaignante sans possibilité pour sa part de départager le vrai du faux.

4. CONCLUSIONS

Le Comité permanent R se pose la question de savoir s'il est justifié - lorsque l'on invoque un avis qui doit fonder une décision d'octroi ou de refus de la nationalité belge - que les autorités compétentes prennent une décision sur la base d'éléments conditionnels qui, comme cela apparaît dans le cas de Madame X, jouent en défaveur du requérant.

Les délais imposés par le législateur sont tels qu'ils ne permettent effectivement pas à la Sûreté de l'État, pour des raisons de manque de temps et de personnel, de traiter des dizaines de milliers de dossiers de naturalisation en y mettant le soin nécessaire.

Le fait que le service (qui est tenu de respecter des délais et qui transmet sont avis à des autorités qui elles-mêmes disposent de peut de temps pour évaluer les cas) ne peut analyser les éléments utilisés, a pour conséquence que tous les demandeurs ne disposent peut-être pas des même chances.

Là où certains vont sans doute pouvoir bénéficier de la procédure rapide d'acquisition de la nationalité belge en l'absence de vérification de leurs antécédents vu la pression des délais, d'autres par contre pourront se voir tout aussi rapidement refuser cette nationalité sur base d'éléments insuffisamment contrôlés.

Madame X ne semble, en effet, ne pas être un cas isolé. Le Comité permanent R a en effet constaté dans d'autres dossiers de même nature, que la manière dont la Sûreté de l'État délivrait des avis en différentes matières à certaines autorités posait des problèmes.

Le nœud de cette problématique est de savoir :

- de quelle manière et auprès de quelles instances des plaintes relatives à d'éventuelles violations de droits pourront être traitées ;

- de quelle manière les droits garantis par la Constitution et par les conventions européennes peuvent le mieux être respectés ;

- comment rendre compatible la confidentialité nécessaire de certaines données avec l'obligation de donner connaissance à la partie lésée des éléments nécessaires à l'exercice de son action en réparation.

Le Comité permanent R a mené une étude sur ce sujet qui est destinée aux ministres compétents et à sa commission parlementaire de suivi.

CHAPITRE 5: RAPPORT SUR L'ENQUETE CONCERNANT LA PLAINTE D'UNE CANDIDATE A LA NATURALISATION A L'EGARD DE L'AVIS FOURNI PAR LA SURETE DE L'ETAT SUR SA DEMANDE DE NATURALISATION

1. OBJET DE LA PLAINTE

Par lettre datée du 2 avril 2003, Madame X a introduit une plainte auprès du Comité permanent R.

Il ressort de ce courrier que Madame X, de nationalité étrangère, vit en Belgique depuis quelques années et qu'elle est mariée à un ressortissant belge. La plaignante aurait introduit une demande de naturalisation belge en 2002. Celle-ci lui aurait été refusée en raison de son appartenance à un mouvement religieux, considéré par la Sûreté de l'Etat comme étant une « organisation sectaire nuisible ».

Madame X reconnaît qu'elle est membre de ce mouvement mais elle conteste formellement que celui-ci soit considéré comme une organisation sectaire nuisible :

La plaignante mentionne en outre qu'elle s'est adressée au « *Centre d'information et d'avis sur les organisations sectaires nuisibles* (C.I.A.O.S.N.)[185] qui se serait déclaré incompétent pour répondre à la question posée.

2. PROCEDURE

Conformément aux articles 33 et 40 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, le Comité permanent R a décidé le 6 mai 2003 d'ouvrir une enquête de contrôle sur la plainte de Madame X.

La plaignante en a été avertie le 7 mai 2003. Le Président du Sénat et le Ministre de la Justice ont été mis au courant de l'ouverture de l'enquête le 8 mai 2003.

Le même jour une apostille a été adressée au Service d'enquêtes du Comité permanent R pour qu'il demande une copie du dossier à la Sûreté de l'Etat .

Le 13 mai 2003, le Service d'enquêtes et le Comité permanent R ont pris connaissance du dossier de l'intéressée à la Sûreté de l'Etat. D'autres documents et informations complémentaires ont été fournis au Service d'enquêtes du Comité permanent R le 5 juin 2003.

Un rapport portant la mention « Diffusion restreinte » a été approuvé le 5 septembre 2003 et transmis à la ministre de la Justice le 1er octobre 2003 ainsi qu'au parlement et au Sénat le 4 novembre 2003.

[185] Organisme créé par la loi du 2 juin 1998.

La ministre de la Justice n'a formulé aucune remarque quant au contenu de ce rapport.

La présente version publique a été approuvée par le Comité permanent R le 8 avril 2004.

3. COMPETENCE DU COMITE PERMANENT R ET PORTEE DE L'ENQUETE

Le Comité permanent R s'est interrogé sur la manière dont il devait aborder la présente plainte. Celle-ci est en effet d'une nature fort différente de celles dont le Comité permanent R a déjà été saisi par d'autres personnes à l'égard desquelles la Sûreté de l'Etat avait communiqué des informations à une autorité policière, judiciaire ou administrative.

Il s'agissait alors de cas dans lesquels le Comité permanent R était invité à se prononcer sur la véracité d'un fait ou sur la manière dont la Sûreté de l'Etat avait rapporté ce fait déterminé au sujet d'une personne, l'information ainsi transmise ayant donné lieu à une décision défavorable à l'égard de la personne concernée (licenciement, refus de naturalisation, etc…).

Dans le cas d'espèce, la plaignante revendique son appartenance à un mouvement à caractère spirituel et religieux et elle demande au Comité permanent R de se prononcer sur la qualité du travail d'information mené par la Sûreté de l'Etat qui, selon elle, a abouti à ce que la qualification de « secte nuisible » soit donnée à ce mouvement.

Pas plus que le Centre d'information et d'avis sur les organisations sectaires nuisibles, le Comité permanent R n'est compétent pour valider ou non un quelconque label officiel de « secte nuisible » qui serait donné à une organisation religieuse. La mission de ce Centre est de rassembler l'information disponible sur ce sujet de la manière la plus objective, transparente et pluraliste possible pour permettre aux autorités responsables et à tout un chacun de se forger sa propre opinion.

Le rôle de la Sûreté de l'Etat est plutôt de détecter la menace potentielle qu'un de ces mouvements pourrait représenter à l'encontre d'un des intérêts visés par l'article 7 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (sûreté intérieure de l'Etat, pérennité de l'ordre démocratique et constitutionnel, etc …).

En l'occurrence, le Comité permanent R s'est estimé compétent pour examiner la manière dont la Sûreté de l'Etat avait recueilli, analysé et diffusé des informations relatives à l'appartenance de Madame X à un mouvement religieux considéré comme sectaire. La question est donc pour lui de savoir si les renseignements recueillis et transmis par ce service étaient suffisamment pertinents, précis, objectifs et vérifiables pour permettre au ministère public de se forger son opinion et de rendre ainsi un avis en bonne connaissance de cause sur la déclaration de nationalité faite par cette personne.

L'enquête devait donc porter aussi bien sur l'atteinte éventuelle que la Sûreté de l'Etat pouvait avoir causé aux droits de la plaignante que sur l'efficacité de ce service (article 1er de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements).

En aucune manière, le Comité permanent R n'est compétent pour émettre un jugement à propos du caractère éventuellement « nuisible » ou « sectaire » du mouvement incriminé, cette appréciation étant de la compétence des autorités politiques ou judiciaires responsables.

4. LES RESULTATS DE L'ENQUETE

Le 13 mars 2002, la plaignante a introduit une déclaration devant l'Echevin de l'Etat civil de sa commune, suivant laquelle elle voulait acquérir la nationalité belge de son mari, conformément à l'article 16 du Code de nationalité belge.

Le dossier concernant la demande de la nationalité belge fut transmis en mars 2002 par le fonctionnaire de l'Etat civil à la Sûreté de l'Etat .

Cette transmission a été faite sur base de l'article 12bis du Code de nationalité belge et de la circulaire du 25 avril 2000 relative à la loi du 1er mars 2000 modifiant certaines dispositions concernant la nationalité belge (M.B. du 6 mai 2000).

Le ministère public demanda en mai 2002, des renseignements complémentaires, plus précisément concernant les activités de l'intéressée et sa fonction précise au sein d'une organisation. Il était également demandé à la Sûreté de l'Etat d'apporter une réponse à la question de savoir si ces activités « pouvaient représenter une menace pour la sécurité nationale, qui constituerait un obstacle à l'attribution de la nationalité belge à l'intéressée ».

Dans sa réponse adressée au Parquet, la Sûreté de l'Etat mentionne que Madame X est connue de ce service pour être membre d'un mouvement qui a fait l'objet de l'enquête parlementaire d'avril 97 « *visant à déterminer une politique pour combattre les pratiques illégales des sectes et des dangers qui en résultent pour la communauté et pour l'individu, en particulier les mineurs d'âge ».*

Dans un avis complémentaire, la Sûreté de l'Etat donne quelques informations sur les activités de Madame X au sein du mouvement incriminé et signale sa volonté d'envoyer sa fille dans une école fondée par le mouvement à l'étranger.

Selon la Sûreté de l'Etat, ces éléments témoignent du fait que l'intéressée a occupé, au sein du mouvement, une certaine position en vue et des responsabilités.

Toutefois, le courrier mentionne également : « cela ne signifie cependant pas que l'intéressée a été mise en cause ou qu'elle représente une menace pour la sécurité nationale ».

Cette dernière observation indique en tout cas une évaluation objective de la Sûreté de l'Etat, tandis qu'il est clair en même temps que la décision finale est du ressort du magistrat compétent.

5. DOCUMENTATION ET INFORMATIONS AU SUJET DU MOUVEMENT CONCERNE

Le Comité permanent R ainsi que son Service d'enquêtes ont, avant et pendant l'enquête, consulté également d'autres sources dans le but d'avoir une vue plus large des buts et du fonctionnement auquel participe la plaignante.

Ces document sont brièvement commentés ci-dessous en insistant sur la définition de « sectes nuisibles » (ce qui représente en fait l'essence de la plainte) et sur les éléments qui concernent spécifiquement le mouvement incriminé.

De très nombreux sites web témoignent de l'implantation du mouvement concerné dans de nombreux pays.

Des sites présentent le mouvement comme promoteur d'une méthode de méditation afin de parvenir à la « Réalisation du Soi » et à développer notre véritable nature. La méditation est un état de conscience où l'attention n'est plus troublée par les pensées. La photo de la personne fondatrice du mouvement est souvent utilisée comme support pour la méditation.

La pratique de cette discipline permet de prendre en charge sa propre santé physique, émotionnelle et mentale. En conséquence, chacun retrouve d'une façon naturelle le désir de mener une vie saine et d'adapter son comportement aux besoins réels de son organisme.

La discipline en question n'est pas une religion mais la réalisation de Soi, auquel elle tend, permet d'accéder à la vérité de toutes les religions d'une autre manière que par l'acceptation des dogmes.

On trouve également sur l'Internet de nombreux sites « anti-sectes » qui dénoncent le mouvement auquel appartient la plaignante comme étant une secte dangereuse. Un tel site livre de nombreux témoignages d'anciens adeptes de la secte qui tendent à contredire les apparences délibérément trompeuses sous lesquelles celle-ci se présente.

Une étude de Madame Rollet, docteur en psychologie à l'Université de Vienne, explique les huit techniques d'influence des individus utilisées par les sectes. Il résulte de ces témoignages que le mouvement incriminé remplit au moins sept des dix critères définis par la commission parlementaire française sur les sectes.

Les faits suivants ont été imputés à ce mouvement dans les conclusions finales de l'enquête parlementaire, qui ont conduit à la classification du mouvement comme secte « nuisible ».

- Conditionnement et auto-hypnose ;
- Pratiques médicales ;
- Arrangement des mariages ;
- Eloignement des enfants – suites judiciaires ;
- Infiltration des milieux scolaires et artistiques.

Selon la vision du Centre d'information et d'avis sur les organisations sectaires nuisibles (C.I.A.O.S.N.), les points sensibles qui amènent à considérer le mouvement incriminé comme une organisation sectaire nuisible, concernent principalement l'absence de libre choix d'un conjoint et l'envoi des enfants dans des écoles extérieures (situées à l'étranger).

Analyse du service d'étude de la Sûreté de l'Etat

La Sûreté de l'Etat est d'avis que l'enseignement, les positions et les pratiques du mouvement doivent faire l'objet d'une attention soutenue ; provisoirement il n'y a cependant pas d'évolution remarquable, en particulier en ce qui concerne l'impact familial/social sur les membres et sur leur famille (mariage, enfants, repli social, etc …).

Un document contenant une description circonstanciée rédigée par le service d'étude a été transmis en mai 2001 au Magistrat national.

Ce document donne un large aperçu de la création et de l'histoire de l'association, de ses structures, de sa doctrine ou de sa philosophie, ainsi que de ses aspects financiers. Il se clôture par la réaction d'ex-membres qui alimentent la thèse selon laquelle le mouvement en question peut être considéré comme une secte. Les annexes à ce schéma idéologique ont une valeur davantage documentaire.

Ce rapport constitue en même temps une sorte de motivation à considérer l'association comme une secte nuisible. Les points retenus sont :

- La manipulation mentale ;
- Les exigences financières envers les adeptes ;
- Les enfants : selon la fondatrice du mouvement, les enfants des adeptes lui appartiennent à l'exclusion des parents, qui ne sont que les concepteurs physiques. Il est conseillé de confier les enfants à partir de 3 ans à l'école du mouvement.
- La rupture avec le milieu social d'origine ;
- L'atteinte possible à l'intégrité physique des adeptes ;
- Le discours antisocial : la fondatrice s'oppose de manière permanente à l'Occident et plus spécifiquement aussi à la Belgique, sans doute parce que le mouvement y rencontre une opposition ;
- L'exploitation des adeptes au profit des dirigeants de l'organisation : les adeptes de tous les pays sont employés à restaurer des immeubles et à en ériger de nouveaux, tous propriétés de la fondatrice. Ils sont également chargés d'aider à leur entretien et de considérer cela comme un honneur de pouvoir le faire pour leur maître spirituel.

6. CONCLUSION

La communication de renseignements par la Sûreté de l'Etat au ministère public concernant Madame X se fonde sur l'article 12 du Code de Nationalité belge et sur la circulaire du 25 avril 2000 relative à la loi du 1er mars 2000 modifiant certaines dispositions concernant la nationalité belge (M.B. du 6 mai 2000).

Le recueil, l'analyse et le traitement des informations par la Sûreté de l'Etat concernant le mouvement auquel la plaignante appartient se fondent sur les articles 7 et 8 de la loi du 30 novembre 1998 organique des services de renseignements et de sécurité.

Selon l'article 7, la Sûreté de l'Etat e.a. pour mission le recueil, l'analyse et le traitement des informations concernant toute activité qui menace ou pourrait menacer la Sûreté de l'Etat intérieure de l'Etat et la pérennité de l'ordre démocratique et constitutionnel.

Pour l'application de l'article 7, est considéré comme une menace ou une éventuelle menace : « toute activité collective ou individuelle déployée dans le pays ou au départ de l'étranger qui peut être en relation e.a. avec des organisations sectaires nuisibles » (article 8).

Dans sa plainte, Madame X ne conteste pas la constatation selon laquelle elle ferait partie du mouvement incriminé. Elle le reconnaît d'ailleurs elle-même. Elle ajoute que ce mouvement est catalogué à tort comme une « secte nuisible » et attribue cela aux informations de la Sûreté de l'Etat qui selon elle « *a effectué un mauvais travail en reprenant des mensonges et des informations inexactes et en arrivant ainsi à un jugement erroné* ».

Il est exact que la Sûreté de l'Etat s'est basée e.a. sur les conclusions de la Commission parlementaire pour décrire le mouvement en question comme « nuisible ». D'autre par, il faut souligner que d'autres documents et informations obtenues e.a. via internet, semblent confirmer ce point de vue et que le C.I.A.O.S.N. maintient jusqu'à nouvel ordre cette position.

L'abondance, la nature et la précision des données dont la Sûreté de l'Etat dispose dans ce contexte, ne permettent pas de suivre l'affirmation de Madame X selon laquelle ce service : « *a effectué un mauvais travail en reprenant des mensonges et des informations inexactes et en arrivant ainsi à un jugement erroné ».*

On peut également estimer sur la base des résultats de la présente enquête, qu'aucun élément n'indique que la Sûreté de l'Etat , dans le cadre de la demande de Madame X aurait donné à l'autorité décisionnelle compétente un avis partial, arbitraire et non objectif.

Le Comité permanent R estime toutefois qu'il aurait été opportun que la Sûreté de l'Etat rappelle dans son avis au ministère public qu'un rapport non classifié avait été précédemment transmis au magistrat national concernant le mouvement auquel la plaignante appartient et ses pratiques sectaires.

Le Comité permanent R pense que cette précision aurait donné, le cas échéant, aux parties concernées par la procédure, la possibilité de tenir un débat contradictoire sur cette question qui touche à l'un des droits constitutionnels fondamentaux qui est la liberté du culte.

D. AVIS DEMANDE PAR

MADAME LA MINISTRE DE LA JUSTICE

AVIS DU COMITÉ PERMANENT R CONCERNANT LE CADRE JURIDIQUE DANS LEQUEL LA SURETE DE L'ETAT ET LE SGRS PEUVENT PROCEDER A DES VERIFICATIONS DE SECURITE SUR DES PERSONNES ET TRANSMETTRE DES AVIS ET INFORMATIONS À CARACTÈRE PERSONNEL AUX AUTORITÉS.

« J'envisage de prendre une initiative législative pour permettre au citoyen d'introduire une réclamation auprès d'une autorité indépendante et mieux préciser la relation entre la Sûreté de l'Etat et les diverses autorités publiques ». (Réponse de la ministre de la Justice à la question n° 357 d'un membre de la Chambre des représentants le 20 octobre 2003 – CRABV 51 COM 024).

1. CONSIDÉRATIONS GÉNÉRALES

La loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité a expressément confié aux services de renseignement belges la mission d'effectuer des enquêtes de sécurité sur les personnes physiques ou morales qui, pour l'accomplissement de certaines tâches d'intérêt public, doivent détenir une habilitation de sécurité. Pour protéger certains intérêts fondamentaux de sécurité du pays, la possession d'une habilitation spéciale peut en effet être requise avant d'accéder à certains emplois, fonctions ou grades (publics ou privés), à certaines informations, documents ou données, à des matériels, matériaux ou matières classifiés, à des locaux, à des bâtiments ou à des sites protégés ou pour l'exécution de certains contrats et marchés publics.

La procédure d'octroi de cette habilitation de sécurité est minutieusement réglée par la loi et un droit de recours existe devant le Comité permanent R dans le cas où l'habilitation ne serait pas octroyée ou serait retirée. Mais , il existe également d'autres situations dans lesquelles une loi ou un usage administratif prescrit qu'un service de renseignement (surtout la Sûreté de l'Etat), soit consulté afin de savoir s'il existe des motifs de sécurité pour refuser ou retirer un droit comme la nationalité belge, une fonction ou une agréation à une personne. Le Comité permanent R a en effet dénombré pas moins de 13 cas de figure dans lesquels il arrive que la Sûreté de l'Etat soit sollicitée par une autre autorité pour délivrer un avis ou une information préalablement à la prise d'une décision individuelle.

Le Comité permanent R a examiné le cadre juridique dans lequel, hormis le cas des habilitations de sécurité, les services de renseignements belges traitaient et transmettaient des informations ou avis d'ordre personnel à d'autres autorités en vue d'une décision à caractère individuel.

Le cas des enquêtes menées pour l'octroi des habilitations de sécurité n'a pas été examiné ici puisque l'exercice de cette mission et le droit de recours sont réglementés par deux lois du 11 décembre 1998. Le Comité permanent R pense que ces procédures légales offrent les garanties de qualité nécessaires pour protéger les droits de la personne, et qu'il n'est donc pas nécessaire de les réformer.

Dans le cadre de cet avis, le Comité permanent R s'est demandé comment, au fil du temps, les droits de la personne avaient été mis en balance par rapport aux intérêts de la sécurité collective. Auparavant, le contrôle social formel, mais surtout informel (avec tous les avantages et les inconvénients qui en découlent) jouait un rôle important dans l'appréciation de la fiabilité d'une personne. Aujourd'hui, le contexte a évolué : la société est devenue plus vulnérable, la mobilité et l'anonymat des personnes ont augmenté.

La protection de la sécurité collective peut donc nécessiter que la loyauté ou la fiabilité d'une personne soit vérifiée avant de lui attribuer la nationalité belge, l'admettre à séjourner dans le pays, lui confier une mission de confiance ou lui permettre d'exercer une profession sensible. Mais cette nécessité ne doit pas aboutir à l'établissement d'un Etat policier dans lequel les menaces contre la sécurité deviendraient un alibi pour sacrifier les libertés et droits fondamentaux du citoyen. La deuxième partie de cet avis proposera donc des balises juridiques destinées à (re)trouver un équilibre entre l'intérêt général et les droits individuels.

Certains cas de vérifications de sécurité ont déjà été examinées par le Comité permanent R, soit d'une manière générale lors d'enquêtes de contrôle, soit à l'occasion de plaintes individuelles :

- l'octroi d'une autorisation de détention ou de port d'arme dans le cadre de la législation sur les armes (cf. rapport annuel 1998, pp. 103-118 – rapport 2000, pp. 69 - 76) ;

- l'octroi du droit d'accès au territoire et de séjour aux ressortissants étrangers (cf. rapport annuel 1999, pp. 64 – 66) ;

- l'octroi de la nationalité belge par naturalisation ou par option (cf. rapport annuel 1999, pp. 67 – 68, rapport annuel 2001, pp. 172 – 177 ainsi que d'autres rapports sur des plaintes individuelles non encore publiés) ;

- l'octroi à des ressortissants étrangers de l'autorisation d'exercer une fonction d'enseignant dans un établissement d'enseignement (cf. rapport annuel 1999, p. 70) ;

- l'octroi d'une autorisation d'exercer une activité dans le secteur du gardiennage (cf. rapport 2003 non encore publié) ;

- l'octroi d'une autorisation d'exercer la profession de détective privé (cf. rapport 2003 non encore publié) ;

- la désignation des membres de l'Exécutif des Musulmans de Belgique (cf. rapport 2001, pp. 111 – 113) ;

- l'octroi du droit d'accès par la société BIAC aux installations de l'aéroport national (cf. un rapport individuel de 2003 non encore publié) : pour chaque personne amenée à travailler dans l'enceinte protégée de l'aéroport national, la société BIAC consulte la Sûreté de l'Etat. Ce service procède à un contrôle de ses fichiers et transmet un simple avis 'positif' ou 'négatif' aux autorités aéroportuaires, sans aucune indication des motifs tirés de sa documentation ;

- l'agréation des membres du personnel de sécurité de l'aéroport national chargés de contrôler l'embarquement des passagers et des bagages ;

- l'octroi à des ressortissants belges ou à des personnes séjournant en Belgique du droit d'immigrer dans certains pays étrangers ;

- l'agréation des membres de services privés de sécurité ou des journalistes dans le cadre des sommets européens à Bruxelles ;

- l'habilitation des membres du personnel de la cellule centrale d'écoutes de la Police fédérale ;

- la désignation des aumôniers musulmans (ou conseillers islamiques) dans les prisons.

Dans certains cas, la consultation du service de renseignement par l'autorité administrative n'est que ponctuelle, c'est-à-dire à l'occasion d'un événement déterminé. Mais dans la plupart des cas, la consultation par l'autorité est récurrente. Au total, on peut estimer à plusieurs dizaines de milliers par an le nombre de consultations effectuées par des autorités auprès des services de renseignement. Il ne s'agit donc pas d'une activité marginale de ces services.

Il arrive par ailleurs que ce soit la Sûreté de l'Etat elle-même qui prenne l'initiative de transmettre des informations d'ordre individuel à une autorité lorsqu'elle estime devoir l'avertir d'une menace potentielle. ([186])

[186] En 2003, le Comité permanent R a transmis au ministre de la Justice et au Parlement un rapport sur le cas de la chanteuse Soetkin Collier. Ce cas individuel a été épinglé par la presse au cours de l'année 2003.

Toutes ces vérifications peuvent porter différentes dénominations telles que « *enquêtes (limitées) », « contrôles »* ou *« vérifications de sécurité », « enquêtes de moralité », « vérifications des antécédents, des relations », « avis », « enquêtes à caractère de sécurité », « enquête d'intégrité »* ou *« de fiabilité », « screening »*, etc. Mais toutes ces appellations désignent en fin de compte le même type d'enquête ou de vérification effectuée au profit d'une autre autorité ([187]) (parfois étrangère [188]), principalement dans l'intérêt de la sécurité nationale ([189]), en vue d'apprécier si une personne offre des garanties suffisantes de fiabilité, de loyauté et de sécurité pour obtenir ou conserver un droit ou l'autorisation d'exercer une fonction à laquelle s'attache une confiance particulière ([190]).

Pour éviter toute confusion avec **l'enquête de sécurité** telle qu'elle est réglementée par la loi du 11 décembre 1998, le Comité permanent R parlera plutôt de « **vérification de données à caractère personnel sur les conditions de sécurité »** ou pour faire bref, de **« vérification de sécurité** » pour désigner toute pratique similaire à l'enquête de sécurité mais non couverte par la loi précitée.

La « vérification » peut inclure tout type de recueil de données à caractère personnel, que ce soit par la simple consultation de sources ouvertes, de fichiers ou de dossiers préexistants (aussi bien les propres fichiers des services de renseignement que ceux d'autres services ou autorités) ou par la mise en œuvre de moyens actifs d'investigation comme la collecte d'informations sur le terrain, l'audition de personnes, l'observation directe, la filature, etc. Mais dans la plupart des cas cependant, une vérification de sécurité se limite à la consultation de fichiers et de données que le service de renseignement a déjà recueillies dans le cadre d'enquêtes menées sur les sujets faisant l'objet de ses missions légales.

---

187 La Sûreté de l'Etat procède aussi à des enquêtes "à des fins domestiques" dans deux cas : pour vérifier la fiabilité d'un candidat informateur d'une part (ce type d'enquête ne sera pas abordé dans le présent avis), deuxièmement, lorsqu'elle doit décider elle-même de l'octroi d'un permis de port d'arme. Le Comité permanent R s'est déjà penché plusieurs fois sur ces situations dans ses rapports annuels; rapport annuel 1999 (77-78) ; Rapport annuel 2000 (70-79).

188 Il arrive en effet que la Sûreté de l'Etat recueille et transmette des informations à des autorités étrangères à propos de personnes (de nationalité belge ou étrangère) qui résident sur notre territoire. C'est notamment le cas pour des personnes qui désirent émigrer au Canada, en Afrique du Sud, en Nouvelle Zélande ou en Australie. C'est aussi le cas lorsque la Sûreté de l'Etat collabore à une enquête de sécurité effectuée par une autorité étrangère dans le cadre d'une convention internationale bi- ou multilatérale (ex. pour l'OTAN, l'UEO, EUROCONTROL, etc.)

189 La sécurité nationale est, selon l'article 8 alinéa 2 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, la première cause de légitimation d'une immixtion dans la vie privée. Mais il est vrai que d'autres raisons justifient aussi la conduite de vérifications de sécurité. Ainsi, lorsque la Sûreté de l'Etat est requise de rendre un avis préalable à l'octroi d'une licence de détective privé, c'est aussi en vue du maintien de l'ordre public, de la prévention d'infractions et de la protection des droits et libertés de tiers.

190 Dans deux cas, des enquêtes de fiabilités peuvent être menées sans que le résultat en soit l'octroi ou le retrait d'un permis ou d'une licence. Il s'agit d'abord des demandes de renseignements adressées par le ministre des Affaires étrangères au sujet des ambassadeurs, attachés militaires et autres diplomates accrédités en Belgique (une centaine de cas par an) pour lesquelles une enquête peut être menée sur le terrain. Le deuxième cas (très exceptionnel) concerne des renseignements demandés au sujet de personnes perturbées mentalement qui sont entrées en contact avec l'une ou l'autre administration. Ce type d'enquêtes ne sera pas abordé dans le présent avis.

Les deux services de renseignement institués par la loi organique du 30 novembre 1998 ne sont d'ailleurs pas les seuls à mener des 'vérifications de sécurité'. D'autres autorités, qu'elles soient administratives ou judiciaires, et même des firmes commerciales, le font aussi, avec ou sans base légale ([191]).

Dans la deuxième partie de cet avis, on tentera de dégager quelques principes légaux essentiels dans lesquels les services de renseignement (et/ou d'autres services) devraient pouvoir mener des vérifications de sécurité. Ces principes seront examinés par rapport aux conclusions tirées d'une réflexion approfondie sur les questions suivantes :

- une vérification de sécurité constitue-t-elle une immixtion dans la vie privée au sens de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 (CEDH) ?

- existe-t-il une ou plusieurs bases légales sur lesquelles cette pratique peut s'appuyer ? Sont-elles suffisantes au sens de cette convention ? Si non, quels éléments devraient compléter la loi (article 22 de la Constitution) ?

- lorsqu'une vérification de sécurité est prescrite par la loi, un service de renseignement peut-il ou doit-il d'office y apporter sa collaboration ou bien cette collaboration doit-elle être prévue explicitement par ou en vertu de la loi (articles 7 et 11 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité) ?

- au sens 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, quelles exigences qualitatives doit-on attendre des informations et des avis transmis à une autorité par les services de renseignement dans le cadre des vérifications de sécurité ?

- ne faut-il pas un contrôle externe sur les vérifications de sécurité ?

- le citoyen dispose-t-il d'un recours (aussi) effectif (que possible) dans le cas où il estimerait que ses droits ont été lésés comme le prévoit l'article 13 de la CEDH ?

- dispose-t-il à cette fin d'un droit d'accès aux données personnelles que les services de renseignement ont communiquées aux autorités ?

- existe-t-il un contrôle externe sur la classification de documents, en particulier lorsqu'il s'agit de données à caractère personnel transmises en vue d'une décision relative à une personne ?

Des recommandations seront formulées sur base des réponses à ces questions.

---

[191] On pense ici aux enquêtes de moralité réalisées par les services de police pour l'octroi d'un certificat de bonne vie et mœurs. Il arrive aussi que des particuliers ou que des entreprises mènent ou fassent mener de telles enquêtes à des fins privées. Ainsi les pre-employment-checks menés par des détectives privés ou des services privés de renseignement (voir rapport de l'enquête « *sur les missions et les activités des services de renseignement officiels à l'égard du renseignement privé* » que le Comité permanent R a finalisée en 2003 et adressé à sa Commission de suivi du Sénat en novembre 2003 pour discussion).

Les réponses aux questions posées ci-avant ont été développées dans une réflexion juridique approfondie menée par le Comité permanent R. Pour aller à l'essentiel, le présent document ne reprend ici que les conclusions qui en ont été tirées.

Conclusion I : Toute vérification de sécurité constitue une immixtion dans la vie privée.

Que ce soit la simple transmission d'informations déjà présentes dans un fichier ou dans une base de données, la simple formulation d'un avis (motivé ou non) ou la recherche d'informations complémentaires, toute vérification de sécurité constitue une immixtion dans la vie privée dont le droit est protégé par l'article 8 de la CEDH et par l'article 22 de la Constitution. Ceci est vrai quel que soit le type de donnée à caractère personnel transmise, que ce soit l'identité, le domicile, l'état civil ou encore des informations touchant la vie privée de la personne soumise à vérification comme son état de santé, sa situation familiale et financière, ses convictions politiques ou religieuses, son mode de vie, etc. Ceci reste vrai quelle que soit la manière dont les informations ont été recueillies (à l'insu ou avec l'accord de l'intéressé) et le caractère confidentiel ou non de leur traitement par le service.

Conclusion II : Les vérifications de sécurité auxquelles les services de renseignement procèdent ne sont pas toutes prévues par une loi qui en détermine les finalités et qui garantit la proportionnalité des moyens par rapport à ces finalités.

«*Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi (…)*» (article 8, alinéa 2 de la CEDH).

Constituant une immixtion dans la vie privée de personnes, toute vérification de sécurité n'est donc permise que si une base légale formelle la prévoit et en détermine préalablement les circonstances ainsi que les conditions (article 22 de la Constitution).

Ainsi par exemple, dans son avis rendu le 12 juin 2003 (n° 30/2003), la Commission de protection de la vie privée déclare que l'enquête de moralité prescrite par circulaire dans le cadre de la délivrance d'attestations de bonne vie et mœurs est contraire à l'article 22 de la Constitution. Il n'existe en effet aucune base légale pour justifier cette immixtion dans la vie privée.
Sans entrer dans le détail, le Comité permanent R estime que la plupart des vérifications de sécurité auxquelles les services de renseignement procèdent ne satisfont pas non plus à cette exigence.

Certaines lois comme la législation sur les armes, celle sur l'accès des étrangers au territoire et le code de la nationalité prévoient cependant que des vérifications à caractère personnel peuvent être effectuées à l'égard des personnes qui sollicitent, qui un permis de port d'arme, qui le droit de s'installer en Belgique ou qui encore la naturalisation belge. Ces vérifications sont généralement effectuées par le ministère public qui consulte à son tour la Sûreté de l'Etat à cet effet.

Mais un cadre légal ne suffit pas pour légitimer une vérification de sécurité. Il faut que la vérification « *constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* ». Ce principe exige aussi que la vérification de sécurité soit proportionnelle à sa finalité légitime. C'est pourquoi le Comité permanent R est d'avis, comme le Conseil d'Etat ([192]),que la loi devrait aussi indiquer la nature des données qui peuvent être recueillies ainsi que les manières dont ces données peuvent être recueillies selon la finalité poursuivie.

Pour le Comité permanent R, ce qui est le plus contraire au principe de proportionnalité de la CEDH, c'est que l'on puisse mener une vérification de sécurité sans en avertir la personne concernée. Lorsque celle-ci postule l'exercice d'un droit ou d'une fonction, l'obtention d'une permission spéciale, elle devrait être en mesure de savoir si la décision d'octroi dépend d'une vérification de données à caractère personnel à son égard. Ce n'est que de cette manière que l'intéressé peut décider librement s'il souhaite obtenir le droit, la fonction ou l'autorisation demandée. Il ne doit pas nécessairement savoir de quelle manière concrète l'enquête sera menée ni quelles informations à caractère personnel seront transmises à l'autorité. Il n'est pas non plus indispensable qu'il sache si une enquête complémentaire est effectivement menée, pourvu qu'il sache qu'une telle enquête peut l'être et de quelle manière (article 22 de la Constitution).

La loi devra donc déterminer de manière suffisamment claire les finalités pour lesquelles un service de renseignement peut procéder à des vérifications de sécurité sur une personne et les conditions dans lesquelles il peut communiquer les informations à caractère personnel qui ont ainsi été recueillies à des autorités.

Conclusion III :

- **la Sûreté de l'Etat ne peut pas effectuer de vérification de sécurité si cette mission ne lui est pas donnée par la loi ou en vertu de la loi,**

- **le SGRS ne peut pas effectuer de vérification de sécurité si cette mission ne lui est pas donnée par la loi.**

[192] Avis du 29 novembre 1995 sur un projet d'arrêté royal relatif à l'enquête de sécurité dans le secteur nucléaire (documents parlementaires, Chambre des représentants, 1996 – 1997, 1193/1 et 1194/1) ; avis du 27 mars 1996 sur une première tentative de donner une base légale aux enquêtes de sécurité (doc. parl. Chambre, 1995 – 1996, 638/1, 34) ; avis du 21 mai 1997 sur un projet relatif aux enquêtes de sécurité (doc. parl. Chambre, 1996- 1997, 1193/1) et avis du 1er février 1999 rendu à l'occasion d'une proposition visant à réformer la loi sur les entreprises de gardiennage (doc. parl. Chambre, 1998 – 1999, 2027/1, 25).

Les articles 7 et 11 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité énumèrent de manière limitative les missions attribuées à ces services. Parmi ces missions figure l'exécution des enquêtes de sécurité conformément aux directives du Comité ministériel du Renseignement et de la Sécurité (art. 7, 2° et 11, 4°). Il ne s'agit ici que des enquêtes de sécurité prévues par la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité. Par ailleurs, la Sûreté de l'Etat peut être chargée « *d'exécuter toutes autres missions qui lui sont confiées par ou en vertu de la loi* » (art. 7, 4°). L'article 11 ne contient pas de disposition similaire pour le SGRS.

A ce jour, il n'existe que deux lois donnant explicitement à la Sûreté de l'Etat la mission de formuler à l'égard d'autres autorités des avis de sécurité à l'égard de personnes, ainsi :

- en matière d'octroi de la nationalité belge, l'article 21 du Code de la nationalité organise la consultation directe de la Sûreté de l'Etat par la Chambre des représentants dans la mise en œuvre de la procédure de naturalisation. Par contre, la communication d'un avis de la Sûreté de l'Etat au ministère public dans le cadre des procédures d'acquisition de la nationalité belge par déclaration, par option ou par naturalisation n'est prévue que par une circulaire ministérielle. Peut-on en déduire qu'il s'agit d'une mission confiée en vertu de la loi ou ne faudrait-il pas un arrêté royal pour la légitimer ?

- l'article 6 bis de la loi du 10 avril 1990 réglementant l'activité des entreprises de gardiennage ou de sécurité ainsi que les services internes de gardiennage prévoit que la Sûreté de l'Etat peut être chargée de mener des enquêtes sur les conditions de moralité auxquelles les responsables et les collaborateurs de ces entreprises doivent satisfaire pour être agréées. Les données examinées ne peuvent être que des renseignements de police judiciaire et/ou administrative et/ou des données professionnelles pertinentes au regard des conditions posées par la loi. La personne qui fait l'objet de l'enquête doit y consentir préalablement.

Un projet de loi modifiant la loi sur les détectives privés prévoit explicitement que le ministre de l'Intérieur devra solliciter l'avis de la Sûreté de l'État avant d'octroyer une autorisation individuelle d'exercer la profession de détective privé (Sénat 3-433/1, 19 décembre 2003).

En matière d'autorisation de détention et de permis de port d'armes, la Sûreté de l'Etat, agissant comme délégué du ministre de la Justice, dispose de pouvoirs décisionnels à l'égard des étrangers et des citoyens belges sans résidence en Belgique. Il s'agit ici d'une mission qu'elle exerce « en vertu de la loi ».
La Sûreté de l'Etat délivre aussi des avis à l'intention des autres instances chargées de l'application de la législation sur les armes, à savoir, les gouverneurs de province, les polices locales et l'Office des Etrangers. En 1998, le Comité permanent R a relevé que le fondement légal et réglementaire de ces avis formulés pour des personnes résidant en Belgique était plus qu'incertain. Une proposition de loi déposée en septembre 2002 a cherché à remédier à cette situation en prévoyant que l'avis de la Sûreté de l'Etat était requis préalablement à toute délivrance d'autorisation de détention ou de permis de port d'arme quel que soit le lieu de résidence du demandeur (Sénat 2-1438/1, 17 septembre 2002). Cette proposition n'a pas abouti.

L'article 19 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ne peut pas être invoqué comme base légale suffisante à la formulation systématique d'avis ou à la communication d'informations de sécurité. Si cette disposition permet bien à un service de renseignement de transmettre des données à certaines autorités publiques, administratives, de police ou judiciaires, et même à des instances ou à des personnes privées, il doit s'agir de « *renseignements visés à l'article 13, deuxième alinéa* », c'est-à-dire de renseignements présentant un lien avec une des menaces que le service a pour mission de surveiller en vertu des articles 7 et 11 de la loi précitée.

Un exemple peut éclairer la différence qui existe entre la compétence de communiquer des renseignements à d'autres autorités dans le cadre de l'article 19 d'une part, et la vérification de sécurité d'autre part.

Si l'attention de la Sûreté de l'Etat a été attirée par une personne parce que celle-ci entretient des contacts avec des milieux extrémistes (compétence définie à l'article 7, 1°), et que cette même personne occupe une fonction sensible dans un aéroport, la Sûreté de l'Etat devra certainement en avertir les autorités aéroportuaires sur base de l'article 19. La situation est toute différente lorsque ces mêmes autorités aéroportuaires interrogent la Sûreté de l'Etat de manière systématique préalablement à la délivrance d'un badge de sécurité à un membre du personnel, sans motif particulier de suspicion à son égard. Ce service ne peut répondre à une telle demande sans en avoir reçu la mission spécifique en vertu d'une loi.

Le Comité permanent R pense que l'article 22 de la Constitution n'impose pas nécessairement au législateur de déterminer les services habilités à effectuer les vérifications de sécurité ni ceux auprès de qui des avis et informations de sécurité peuvent être recueillis. Le plus souvent, la description des données que le législateur estime relevantes pour l'appréciation d'un dossier suffira à déterminer auprès de quel service on peut s'adresser.

Par ailleurs, si le législateur désigne expressément certaines autorités ou certains services pour effectuer ces vérifications, délivrer des avis ou communiquer des informations de sécurité, la question se pose alors de savoir si le pouvoir exécutif est encore compétent pour désigner d'autres services. Ce problème dépasse les services de renseignement.

Mais si on veut confier à la Sûreté de l'Etat l'exécution d'autres enquêtes ou vérifications de sécurité que celles prévues par la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité, il faudra bien plus qu'une directive du Comité ministériel du Renseignement et de la Sécurité pour légitimer cette mission.

Le Comité permanent R estime donc qu'une <u>loi est nécessaire,</u>

- soit pour confier explicitement la mission à la Sûreté de l'Etat ;

- soit pour la confier au ministre de la Justice ou à son délégué ; dans ce cas, une simple instruction ministérielle devrait compléter la loi ;

- soit pour laisser au Roi le soin de désigner la ou les autorités compétentes pour exécuter la mission; dans ce dernier cas de figure, il faudrait un arrêté royal d'exécution de la loi.

Par ailleurs, l'article 11 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité n'a pas prévu que le SGRS pouvait, comme la Sûreté de l'Etat, être chargé « *d'exécuter toutes autres missions qui lui sont confiées par ou en vertu de la loi* ». Cette situation ne peut certes pas empêcher le législateur de confier une nouvelle mission au SGRS, mais elle s'oppose actuellement à ce que ce service procède à toutes autres vérifications de sécurité que celles prévues par la loi en vue de l'octroi d'une habilitation de sécurité.

<u>Conclusion IV</u> : Les données à caractère personnel communiquées par les services de renseignement dans le cadre d'une vérification de sécurité doivent être aussi sûres, correctes, adéquates et pertinentes que possible. Elles doivent être non excessives au regard des finalités de sécurité. Elles doivent donc pouvoir être vérifiables et vérifiées dans le cadre d'un contrôle externe et d'un droit de recours.

Certains principes essentiels de la loi sur le traitement des données à caractère personnel s'appliquent à toutes les données, classifiées ou non, recueillies et traitées par les services de renseignement. Ainsi ces données doivent avoir été collectées pour des finalités en rapport avec leurs missions légales. Les données doivent aussi être adéquates, pertinentes et non excessives au regard de ces finalités. Elles doivent enfin être exactes, donc vérifiées et si nécessaires, mises à jour, ce qui signifie que toutes les mesures raisonnables doivent être prises pour effacer ou corriger les données imprécises ou inexactes par rapport aux objectifs pour lesquels elles ont été recueillies.

Le Comité permanent R est d'avis que cette disposition oblige les services de renseignement à ne point transmettre d'information à caractère personnel vers une autorité extérieure sans l'avoir validée et mise à jour, en procédant, le cas échéant, à une enquête complémentaire.

Ceci ne doit pas avoir pour résultat d'obliger ces services de ne communiquer que des informations certaines à 100 %, surtout en cas de risque grave de sécurité. Mais l'esprit de la loi requiert alors que le service de renseignement indique quel est le degré de certitude de l'information communiquée, surtout s'il existe des motifs de douter de la source, de l'exactitude ou de la précision de certaines données. S'agissant d'informations à caractère personnel, il est capital que le service de renseignement vérifie l'exactitude de toutes les données d'identité de la personne physique concernée et qu'il prenne toutes les mesures adéquates afin de détecter et de signaler d'éventuelles homonymies.

<u>Conclusion V</u> : L'exécution de vérifications de sécurité par les services de renseignement doit être contrôlée par un organe de contrôle extérieur et indépendant.

Au sens de l'article 8 de la CEDH, au plus la sécurité nationale ([193]) est en danger, au moins d'exigences sont posées en terme de prévisibilité de la réglementation légale (pour savoir notamment quelles données peuvent être recueillies et transmises aux autorités. Mais au plus s'imposent alors des garanties adéquates et effectives contre les abus. Ces garanties doivent être confiées à un organe disposant d'un réel pouvoir de décision.

Mais le Comité permanent R pense que l'existence d'un organe décisionnel indépendant et impartial n'est pas suffisante pour ériger un contrôle adéquat et effectif. Il est aussi essentiel, pour qu'un contrôle soit efficace, que cette instance dispose, non seulement d'une compétence juridique d'appréciation (et donc d'une bonne connaissance juridique des diverses réglementation en jeu), mais aussi d'une bonne connaissance des service de renseignement eux-mêmes, de leurs méthodes de travail, de leurs champs d'action, des menaces et des conditions opérationnelles dans lesquelles ils doivent travailler.

Il est aussi essentiel que l'instance de contrôle dispose aussi d'un droit d'initiative pour évoquer les dossiers. Si celle-ci ne peut agir que sur recours d'un citoyen (qui ne sait pas toujours que des données sont recueillies à son égard et qu'elles sont communiquées), il n'y a pas de véritable contrôle.

Le Comité permanent R pense également que dans certains cas, un contrôle effectif n'est possible que si le service contrôlé est obligé de communiquer spontanément certains cas ou incidents à l'instance de contrôle. De plus, l'organe de contrôle doit avoir accès à tous les documents et pouvoir entendre les membres des services de renseignement déliés pour cette circonstance de leur devoir de secret professionnel ([194]). Enfin, il est important que ce service dispose à cet effet de moyens suffisants en personnel et en logistique.
Dans ce cadre législatif actuel, cinq instances fédérales différentes peuvent exercer des compétences de contrôle ou de recours à l'égard des avis de sécurité formulés par les services de renseignement, à savoir le Conseil d'Etat, la Commission d'accès aux documents administratifs (la CADA), les médiateurs fédéraux ([195]), la Commission de protection de la vie privée, et le Comité permanent R. Ces instances sont investies chacune de missions et de compétences en partie redondantes et en partie, complémentaires. En effet :

---

193 Ou l'un des autres intérêts cités dans l'alinéa 2, comme la sûreté publique, le bien-être économique du pays, la défense de l'ordre et la prévention des infractions pénales, la protection de la santé ou de la morale, ou la protection des droits et libertés d'autrui.

194 Voir par exemple les articles 48 à 51 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

195 Les rapports annuels des médiateurs fédéraux indiquent que ceux-ci ont traité trois plaintes impliquant la Sûreté de l'Etat au cours de ces trois dernières années.

- certaines de ces instances peuvent contrôler le fonctionnement global des services de renseignement, d'autres ne sont compétentes que pour un aspect de leurs missions seulement : Ainsi, le Comité permanent R contrôle le fonctionnement général des services de renseignement tandis que la Commission de protection de la vie privée ne peut examiner leur fonctionnement que du point de vue du respect de la loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Cette Commission ne peut pas examiner d'autres plaintes individuelles que celles relatives à cette matière.

- certaines instances, comme le Comité permanent R, peuvent prendre des initiatives dans certains domaines, d'autres doivent attendre le recours d'un citoyen ou la demande du parlement pour agir; parfois, ces deux possibilités sont combinées.

- certaines instances, comme le Comité permanent R, peuvent se rendre sur place ou mieux, exiger l'accès à tous les locaux, d'autres ne disposent pas de cette possibilité ([196]).

- les unes, comme le Comité permanent R, peuvent désigner des experts, les autres non ou seulement, dans quelques cas bien déterminés.

- les unes peuvent parfois procéder à l'audition de membres de services de renseignement (cas dans lequel il n'est pas toujours établi si ceux-ci peuvent invoquer le secret professionnel), les autres peuvent même parfois faire procéder à une citation ([197]).

- tel organe peut consulter tout document, l'autre peut exiger la communication de tout document et même, imposer une astreinte.

- dans telle circonstance, un organe de recours a le pouvoir de prendre une décision contraignante (le Conseil d'Etat ou le Comité permanent R en matière d'habilitation de sécurité), dans telle autre, l'organe de contrôle se limite à rédiger un rapport (public ou confidentiel), à rendre un avis ou à émettre des recommandations.

Dans ce contexte, il n'est pas toujours aisé de comprendre les rapports entre toutes les dispositions légales qui organisent les contrôles et les recours des citoyens concernés par une vérification de sécurité : telle loi est-elle une *lex specialis* par rapport à une autre ou pas ? Si l'on ajoute à ce débat la problématique de la classification des documents, il devient alors très difficile de savoir globalement et concrètement qui peut faire quoi.

Il est donc permis de se poser des questions sur l'effectivité d'un système de contrôle des vérifications de sécurité qui serait dispersé entre plusieurs instances.

---

196 Dans ce cadre, la CADA ne dispose d'aucune de ces prérogatives.

197 C'est ici que les moyens d'investigation du Comité permanent R vont le plus loin : celui-ci peut faire citer les membres des services de renseignement par huissiers de justice. Ces membres ne peuvent se retrancher derrière leur devoir de secret professionnel (articles 48 à 51 de la loi du 18 juillet 1991).

Conclusion VI : Le citoyen qui fait l'objet d'une vérification de sécurité par un service de renseignement doit disposer d'un droit de recours auprès d'une instance indépendante disposant d'un réel pouvoir de décision en la matière.

L'article 13 de la convention européenne des droits de l'homme requiert que le citoyen dispose d'un moyen de droit auprès d'une instance nationale compétente qui lui permette de faire examiner toute plainte relative à une violation d'un droit fondamental et de demander une réparation appropriée si la violation est avérée. Cette instance ne doit pas nécessairement appartenir à l'ordre judiciaire mais il faut que ses compétences et que les garanties de procédure rendent le moyen effectif. Il faut néanmoins souligner que la jurisprudence de la Cour européenne des droits de l'homme fixe la barre plus bas lorsque le maintien du secret est requis, tout comme en matière de 'prévisibilité'. Il faut alors examiner si tous les moyens pris dans leur ensemble suffisent à offrir la meilleure réparation possible.

Vu que la plupart des vérifications de sécurité servent à préparer et à justifier des actes administratifs (à l'exception des naturalisations), c'est au Conseil d'Etat d'apprécier la légalité de ces décisions. C'est d'ailleurs de cette manière qu'actuellement un avis erroné ou sans nuance, rendu par un service de renseignement, peut être attaqué, du moins indirectement, en vue d'une réparation appropriée.

Le contrôle du Conseil d'Etat ne s'étend pourtant pas aux décisions des autorités de sécurité en matière d'octroi des habilitations de sécurité. En cette matière, c'est le Comité permanent R qui agit en qualité d'organe de recours. Cette compétence d'organe de recours pourrait être étendue à toutes les autres vérifications des conditions personnelles de sécurité auxquelles procèdent les services de renseignement.

Conclusion VII : Dans l'état actuel de la législation, les voies offertes au particulier pour vérifier les données personnelles dont les services de renseignements disposent à son égard sont dispersées mais restent dans la plupart des cas peu opérantes.

Pour pouvoir exercer son recours avec quelque chance de succès, il est évident que le requérant doit pouvoir prendre connaissance de l'avis et des données à caractère personnel que le service de renseignement a transmis à l'autorité le concernant. La question de l'accès du particulier aux informations recueillies à son égard par un service de renseignement est très délicate et doit être abordée avec beaucoup de prudence. Cette problématique a déjà été examinée par le Comité permanent R en 1997 ([198]).

[198] Comité permanent R, rapport d'activités 1997, pages (54 et suiv. NL)

La plupart des renseignements communiqués aux autorités par les services de renseignement sont des informations tirées de sources ouvertes et/ou de registres officiels (par exemple, le casier judiciaire) et peuvent donc, en principe, être portés à la connaissance des parties concernées. Mais les informations les plus sensibles (par exemple, celles qui font état d'activités clandestines) sont souvent classifiées soit en raison de la protection des sources humaines (ou techniques lorsque la loi le permet), soit de la protection des intérêts fondamentaux de l'Etat. Il s'agit d'éléments recueillis dans le cadre d'un travail de collecte d'informations qui ne peuvent être communiqués qu'aux seules personnes titulaires d'une habilitation de sécurité ainsi qu'aux magistrats.

La plus grande prudence s'impose donc dans le traitement et la communication de ces informations, surtout si elles sont unilatérales et qu'elles ne peuvent être ni vérifiées, ni soumises à contradiction.

Le Comité permanent R a examiné différentes procédures qui peuvent avoir pour objet ou pour effet d'ouvrir aux particuliers un accès direct ou indirect aux données à caractère personnel que les services de renseignements disposent sur eux et de les contester. Dans l'état actuel de la législation, seule la procédure de recours prévue dans le cadre de la loi sur la classification et les habilitations de sécurité semble offrir à un particulier un droit effectif d'accès au dossier de l'enquête qui le concerne.

La Commission de la protection de la vie privée.

Une possibilité d'accès résulte de l'article 13, alinéa 2 de la loi du 8 décembre 1992 sur la protection de la vie privée. Toute personne justifiant de son identité a le droit de s'adresser sans frais à la Commission de la protection de la vie privée pour exercer son droit de consultation et de rectification à l'égard des traitements gérés par l'administration de la Sûreté de l'Etat ou par le Service général du Renseignement et de la Sécurité. Ce recours ne donne toutefois qu'un droit d'accès indirect puisque l'alinéa 3 de l'article 13 précité énonce que : *"La Commission de protection de la vie privée communique uniquement à l'intéressé qu'il a été procédé aux vérifications nécessaires"*.

La loi relative à la publicité de l'administration et la Commission d'accès aux documents administratif.

Une autre possibilité résulte des articles 4 et 5 de la loi du 11 avril 1994 relative à la publicité de l'administration. La Constitution et cette loi du 11 avril 1994 instaurent à cet égard le principe selon lequel la publicité et le droit d'accès aux actes administratifs est la règle, la confidentialité l'exception. Il existe cependant des motifs d'exception obligatoires qui permettent à l'autorité de refuser la communications de certaines informations.

Ces motifs d'exception doivent être appréciés au cas par cas par une mise en balance de l'intérêt de la publicité avec l'intérêt de sécurité en cause. Il existe aussi des motifs d'exception obligatoire par nature, parmi lesquels on peut ranger tout type d'information classifiée ainsi que d'autres types d'informations pour lesquelles il existe une obligation de secret spécifique prévue par une loi particulière, ainsi par exemples, les secrets nucléaires, les secrets militaires de fabrication, les secrets statistiques, le devoir de secret auquel sont tenus les membres des services de renseignement, etc. Il existe enfin des motifs d'exception facultatifs pour lesquels une plus grande marge d'appréciation est laissée à l'autorité. La loi sur la publicité de l'administration dispose que la Commission d'accès aux documents administratifs peut rendre un avis à l'occasion d'une "demande de reconsidération" d'un refus de communication. Cet avis ne lie pas l'autorité administrative fédérale. Un second refus ou l'absence de décision sur une demande de reconsidération peut faire l'objet d'un recours au Conseil d'Etat (art. 8, § 2, 4ème alinéa).

Face à des demandes d'accès de particuliers à leur dossier, la pratique des services de renseignement est de considérer qu'une telle demande se heurte à un des motifs d'exception obligatoire prévus par la loi du 11 avril 1994 sur la publicité de l'administration ou par la loi du 11 décembre 1998 sur la classification et les enquêtes de sécurité ([199]).

C'est souvent le secret de l'identité de la personne qui a communiqué l'information à titre confidentiel (la protection de la source) ou la vie privée d'une tierce personne qui est invoqué comme motif d'exception. Les services de renseignement refusent donc de manière quasi systématique de donner accès à ces informations. Il faut en effet être conscient du fait que la simple prise de connaissance, même partielle, d'un dossier ou d'un avis d'un service de renseignement, pourrait permettre à la personne concernée de connaître la source de l'information et la manière dont elle a été obtenue. Ceci pourrait par ailleurs mettre en péril le fonctionnement et l'efficacité du service et par voie de conséquence, l'un des intérêts qu'il est chargé de protéger.

Les médiateurs fédéraux.

Une possibilité est aussi offerte au citoyen de s'adresser aux médiateurs fédéraux. Leur compétence légale d'examiner des plaintes de citoyens s'étend en effet à toutes les administrations fédérales du pays, y compris la Sûreté de l'Etat et le SGRS malgré la compétence spéciale du Comité permanent R.

La manière dont les médiateurs fédéraux rendent compte aux plaignants de leurs constatations et avis sur le recueil et le traitement d'informations à caractère personnel par les services de renseignement n'est pas encore connue du Comité permanent R.

L'accord de Schengen.

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

---

[199] Voir Comité permanent R : « les devoirs de secret auxquels sont tenus les membres des services de renseignement », étude en annexe du rapport d'activités 1998.

Le recours au tribunal de première instance dans le cadre d'une procédure d'acquisition de la nationalité belge.

Comme on l'a vu plus haut, le Code de la nationalité prévoit l'intervention de la Sûreté de l'Etat dans le cadre des procédures d'acquisition de la nationalité belge, que ce soit par déclaration, par option ou par naturalisation. Selon ces dispositions, le procureur du Roi peut émettre un avis négatif sur la procédure en présence « d'un empêchement résultant de faits personnels graves » concernant la personne en cause. Cet avis, qui doit être motivé, peut se fonder notamment sur des observations préalablement transmises par la Sûreté de l'Etat. L'avis négatif du procureur du Roi peut alors être soumis par la personne concernée au tribunal de première instance qui est ainsi chargé de statuer sur le bien-fondé de l'avis. Un appel peut en outre être interjeté devant la Cour d'appel. Le requérant dispose bien sûr de la possibilité de faire valoir ses arguments à l'encontre de l'avis négatif émis par le procureur du Roi, éventuellement motivé par des informations (classifiées ou non) transmises par la Sûreté de l'Etat.

Le recours en annulation au Conseil d'Etat contre une décision administrative motivée par une information à caractère personnel transmise par un service de renseignement.

Il s'agit par exemple des recours introduits par des personnes à qui un ordre d'expulsion du territoire a été adressé ou à qui l'autorisation d'exercer une activité de gardiennage ou la profession de détective privé a été refusée sur base d'un avis négatif de la Sûreté de l'Etat.

Le Comité permanent R note que la jurisprudence du Conseil d'Etat n'est pas encore constante en ce qui concerne la manière d'appréhender les informations communiquées par la Sûreté de l'Etat pour servir de base à une décision administrative. Deux arrêts récents illustrent deux attitudes différentes à cet égard : l'arrêt n° 102.788 du 23 janvier 2002 et l'arrêt n° 103.016 du 30 janvier 2002.

Dans le premier cas (arrêt n° 102.788), il s'agissait d'une demande d'annulation d'un arrêté ministériel portant refus de renouvellement de l'autorisation d'exercer la profession de détective privé. Cette décision avait été prise notamment sur base d'informations communiquées par la Sûreté de l'Etat au ministre de l'Intérieur faisant état de l'appartenance du détective concerné à une organisation d'extrême droite et de propos antisémites attribués à l'intéressé. Le requérant contestait ces arguments. Le Conseil d'Etat a estimé que les activités et les faits rapportés par la Sûreté de l'Etat, susceptibles de constituer un danger pour l'ordre public ou pour la sûreté de l'Etat, devaient être dûment prouvés et clairement établis. En l'espèce, le Conseil d'Etat a estimé que l'on ne pouvait se satisfaire des renseignements imprécis qui avaient été communiqués par la Sûreté de l'Etat sans indication de sources.

Dans l'autre cas, (arrêt n° 103.016), il s'agissait d'une demande de suspension en extrême urgence d'une décision d'exclure un ressortissant étranger de la procédure de régularisation de séjour sur le territoire du Royaume. Cette décision avait été prise notamment sur base d'informations communiquées par la Sûreté de l'Etat selon lesquelles le demandeur était connu pour son militantisme radical dans la défense de l'instauration d'un Etat religieux intégriste, opposé à la démocratie occidentale et à l'intégration des immigrés musulmans dans leur société d'accueil. Le requérant affirmait ne jamais avoir accompli d'acte délictueux et contestait avoir publiquement exprimé les opinions qu'on lui prêtait. Il faisait valoir que le rapport de la Sûreté de l'Etat, inconnu de lui et de la Commission de régularisation, n'avait pu faire l'objet d'un débat contradictoire. Dans cette affaire, le Conseil d'Etat n'a pas examiné la valeur probante du rapport de la Sûreté de l'Etat. Il a estimé que le ministre, disposant d'un pouvoir d'appréciation pour évaluer le danger pour l'ordre public, pouvait prendre en compte des comportements non délictueux rapportés par la Sûreté de l'Etat pour prendre sa décision, qu'une telle décision n'avait d'ailleurs pas de caractère juridictionnel parce que liée à des questions de sécurité et qu'elle pouvait aussi être prise sans débat contradictoire.

Le Comité permanent R agissant en qualité d'organe de contrôle des services de renseignement.

Une possibilité résulte d'une décision que pourrait prendre le Comité permanent R de rendre public, en tout ou en partie, un de ses rapports d'enquête de contrôle impliquant par-là que ce document puisse être aussi communiqué au plaignant qui a déclenché cette enquête. Sous réserve des données classifiées, ce rapport public pourrait par exemple indiquer que des données à caractère personnel erronées ont été recueillies et/ou communiquées par un service de renseignement au détriment d'un droit ou d'une liberté du plaignant. Néanmoins, la communication d'un avis ou d'un rapport du Comité permanent R suite à la plainte d'un particulier n'est pas explicitement prévue par la loi organique du contrôle des services de police et de renseignement. Cette lacune législative laisse subsister un vide et un doute sur la manière dont le Comité permanent R peut ou doit informer les plaignants à propos de la manière dont leurs droits ont été respectés ou non par les services de renseignement. Dans certains cas, et sous certaines conditions, le Comité permanent R a déjà communiqué ses conclusions aux plaignants.

Le Comité permanent R agissant en qualité d'organe de recours en matière d'habilitation de sécurité.

Une possibilité est prévue par l'article 6 de la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitation de sécurité. Dans le cadre d'un recours, le requérant et son avocat peuvent en effet consulter au greffe du Comité permanent R le rapport d'enquête et, le cas échéant, le dossier d'enquête, Toutefois, à la demande du service de renseignement et de sécurité, le Comité permanent R peut décider de conserver secrètes et de retirer du dossier certaines informations en vue de protéger les sources, la vie privée de tiers ou l'accomplissement des missions des services de renseignement. Lorsque ces informations proviennent d'un service de renseignement étranger, la décision de non-consultation est prise par le service de renseignement et de sécurité. Ces décisions ne sont susceptibles d'aucun recours.

Cette multiplicité de voies administratives et judiciaires peut donc entraîner des problèmes de compétence entre les différentes instances. Ainsi la Commission d'accès aux documents administratifs (CADA) a d'abord estimé que l'intéressé devait d'abord s'adresser à la Commission de protection de la vie privée. Le Conseil d'Etat était plutôt d'avis que la loi sur la publicité de l'administration devait s'appliquer. La CADA a récemment adapté sa jurisprudence administrative dans ce sens mais celle-ci prête à discussion.

Par ailleurs, il peut arriver que l'intéressé ne soit même pas au courant que l'autorité a rendu une décision le concernant sur base d'une information transmise par un service de renseignement si la motivation de cette décision n'y fait pas référence.

En l'absence de procédure unique sur les vérifications de sécurité, à qui doit donc s'adresser le citoyen qui s'estime lésé par la communications à un service de données personnelles recueillies à son sujet par un service de renseignement ? On peut ainsi comprendre qu'il soit déjà arrivé qu'une personne ait adressé la même plainte à plusieurs organes de contrôle en même temps (par exemple au Comité permanent R et la Commission de protection de la Vie privée). Le Comité permanent R n'a pas connaissance de cas où deux organes différents, saisis du même problème, auraient rendu des avis ou des décisions contradictoires, mais cette situation ne peut être exclue en théorie vu qu'il n'existe, ni procédures de concertations, ni d'organe chargé de veiller à l'unicité d'une jurisprudence en matière de vérification de sécurité.

<u>Conclusion VIII</u> : Dans l'état actuel des procédures administratives et judiciaires, la classification des documents et données à caractère personnel n'est soumise à aucun contrôle extérieur et indépendant.

Compte-tenu de son expérience acquise dans l'examen des recours en matière d'habilitations de sécurité, le Comité permanent R a pourtant acquis la conviction que la plupart des demandes d'accès à des données personnelles recueillies par des services de renseignement pourraient être prise en considération après une mise en balance des intérêts en cause, à savoir l'intérêt du particulier et l'un des intérêts de sécurité générale visés par la loi. Dans la majorité des cas, les services de renseignement ne disposent à propos des particuliers que de données tirées de fichiers administratifs, de fichiers de police ou de sources ouvertes, cas dans lesquels la protection de la source ne s'impose pas. Le Comité permanent R reste cependant convaincu qu'il existe bien des situations dans lesquelles la communications de données peut se révéler problématique, notamment dans les cas d'informations classifiées.

Le Comité permanent R estime donc que le maintien du secret sur certaines informations à caractère personnel transmises aux autorités doit être assorti d'un contrôle strict d'un organe extérieur et indépendant sur la classification et sur la motivation du secret. Les membres de cet organe devraient eux-mêmes disposer d'une habilitation de sécurité pour être nommés à cette fonction.

Conclusions générales.

En matière de vérification de sécurité, seule la législation sur le recours en matière d'habilitation de sécurité offre au citoyen concerné une garantie juridique adéquate et effective. En cette matière, le Comité permanent R agit en effet comme organe de recours externe et indépendant.

Dans la plupart des cas, la manière dont les services de renseignement délivrent aux autorités d'autres avis et données à caractère personnel à des fins de sécurité n'est pas conforme à la législation interne et au droit international.

Il convient donc de légiférer en la matière.

2. RECOMMANDATIONS

Si l'on veut développer (pour les différentes sortes de vérifications de sécurité) un système légal adéquat, qui soit tout à la fois, complet, praticable et conforme aux exigences de la CEDH et de la Constitution, le Comité permanent R recommande de répondre à un certain nombre de questions stratégiques. La réponse à la première question déterminera la réponse à la deuxième question, et ainsi de suite.

La première question a trait aux vérifications de sécurité en général, quelle que soit l'implication d'un service de renseignement dans ce type d'enquête. C'est la question de savoir dans quels cas l'autorité veut subordonner l'octroi ou le maintien d'un droit, d'un avantage, d'une fonction ou d'une autorisation à un degré plus élevé de certitude quant à la fiabilité d'une personne en faisant procéder à une vérification plus approfondie de sécurité.

La deuxième question est de savoir sur quels types de données personnelles on peut se baser pour apprécier la fiabilité d'une personne et jusqu'à quel(s) niveau(x) d'investigation la vérification de sécurité devra être menée sur celle-ci en fonction du droit, de l'avantage, de la fonction ou de l'autorisation à lui conférer.

C'est seulement après avoir répondu à ces questions, que l'on pourra alors se demander si la Sûreté de l'Etat est bien le service approprié pour enquêter sur ces matières et participer à la formulation d'avis sur la fiabilité de personnes (troisième question).

La quatrième question est celle de savoir quel degré de transparence on souhaite conférer aux données des services de renseignement. Selon la réponse, il faudra prévoir un organe de contrôle adéquat et effectif et donner à une instance nationale la compétence d'offrir une réparation aussi effective que possible.

2.1. Dans quels cas l'autorité doit-elle subordonner l'octroi ou le maintien d'un droit, d'un avantage, d'une fonction ou d'une autorisation à un degré plus élevé de certitude quant à la fiabilité d'une personne en faisant procéder à une vérification plus approfondie de sécurité ?

Avant d'examiner si nos services de renseignement ont un rôle à jouer en matière de vérification de sécurité, l'autorité doit se fixer une ligne de conduite claire à propos des droits, avantages, fonctions ou autorisations dont l'octroi est subordonné à une vérification de la fiabilité de la personne. En d'autres termes, il s'agit de définir ces droits, avantages, fonctions ou autorisations pour l'exercice desquels l'autorité est en droit de vérifier de manière active, c'est-à-dire par une enquête, la fiabilité des titulaires.

A cet égard, le Comité permanent R ne peut se défaire de l'impression qu'il n'existe pas de ligne de conduite systématique dans le choix des secteurs pour lesquels une vérification de sécurité est nécessaire ou pas[200].

On constate par exemple que le personnel de l'aéroport national est soumis à une vérification de sécurité (screening) alors que celui des aéroports régionaux ne l'est pas. Qui plus est, les membres du personnel des firmes privées de gardiennage qui effectuent les contrôles de sécurité à l'aéroport national sont soumis à une enquête de sécurité approfondie alors que cela ne semble pas être le cas pour le personnel de surveillance des aéroports régionaux et des lignes TGV, en ce compris l'Eurostar vers la Grande Bretagne. Indépendamment du problème éventuel de sécurité que cela suscite, on crée ici une forme d'inégalité entre citoyens.

Cette inégalité se retrouve aussi dans les vérifications de sécurité (screening) des aumôniers de prison du culte musulman : les aumôniers musulmans sont, en effet, soumis à une enquête alors que ceux des autres cultes reconnus, de même que les conseillers laïcs, ne le sont pas.

Il existe par ailleurs des secteurs pour l'accès desquels aucune enquête n'est requise alors que l'exercice de ces fonctions suppose de la part de l'autorité une exigence de confiance élevée à l'égard des personnes qui les exercent. On peut citer par exemples le cas des directeurs de prison ou de centres fermés pour illégaux, des officiers et hauts fonctionnaires de police, des magistrats, etc… .

Il appartient donc aux autorités des secteurs concernés de faire le nécessaire. En tout état de cause, il est nécessaire de définir clairement le rôle, même limité, des services de renseignement dans la réglementation des procédures. Sans cela, toute intervention d'un service de renseignement demeurera un risque tant pour le service lui-même que pour l'autorité politique.
Des exemples récents l'ont hélas démontré.

[200] L'étude du Comité permanent R se limite aux vérifications de sécurité exécutées par l'un des deux services de renseignement. Il va de soi que si l'autorité veut réglementer ces enquêtes de manière globale, elle doit adopter une perspective plus globale.

Le Comité permanent R insiste à nouveau sur le fait qu'il ne souhaite absolument pas l'avènement d'un Etat policier. Une politique bien réfléchie ne doit pas en effet aboutir à mener plus d'enquêtes. Le Comité permanent R pense, par exemple, qu'au sein de l'armée, où des milliers d'enquêtes de sécurité sont réalisées chaque année, on a parfois tendance à exiger trop rapidement une habilitation de sécurité.

2.2. Une fois établis les droits, avantages, fonctions ou autorisations pour l'exercice desquels l'autorité est en droit de s'assurer de la particulière fiabilité des titulaires, il faut se demander :

Sur quels types de données personnelles peut-on se baser pour apprécier la fiabilité d'une personne ?
Jusqu'à quel(s) niveau(x) d'investigation la vérification de sécurité doit-elle être menée pour rechercher ces données personnelles et obtenir ainsi un degré plus élevé de vérification de la fiabilité en fonction du droit, de l'avantage, de la fonction ou de l'autorisation à conférer ?

Cette double interrogation pose la question de l'objet même de l'enquête et des moyens à mettre en œuvre pour recueillir l'information requise. Comme pour les enquêtes réalisées en vue d'obtenir une habilitation de sécurité d'un niveau confidentiel, secret ou très secret, on peut supposer que la recherche de données à caractère personnel sera plus ou moins intrusive dans la vie privée de la personne concernée en fonction du niveau de confiance attaché à la fonction qu'elle exerce ou souhaite exercer. Ce niveau d'exigence quant au degré de confiance doit aussi dépendre de l'ampleur de l'atteinte qui peut résulter d'un abus éventuel du droit, de l'avantage, de la fonction ou de la prérogative. Dans certains cas (par exemple pour les documents très secrets), ce niveau de garanties sera très élevé, dans d'autres (documents confidentiels), il sera plus limité.

L'objet de l'enquête est de déterminer si la personne considérée présente par sa personnalité, son comportement, ses opinions, sa situation familiale, pécuniaire ou professionnelle, un risque potentiel pour la sécurité du pays ou de l'organisation dans laquelle elle est appelée à exercer telle fonction de confiance.

Définir les moyens de collecter l'information à caractère personnel, c'est principalement déterminer les sources qui pourront être consultées ou non pour dresser le portrait du sujet de l'enquête (le casier judiciaire, le registre national, des fichiers de police, les enquêtes de voisinage, dans le milieu professionnel, l'observation directe, etc.)

Le Comité permanent R recommande que chacune des questions de cette problématique soit ainsi examinée de manière systématique et résolue dans la perspective de mettre en place une base légale conforme à l'article 22 de la Constitution.

2.3. Les services de renseignement sont-ils les mieux placés pour émettre des avis (ou participer à la formulation d'avis) dans le cadre de vérifications de sécurité.

Cette question se divise en trois sous-questions :

- ***Les données dont les services de renseignement disposent normalement, sont-elles relevantes en matière de vérification de sécurité ?***

S'il suffit à l'autorité que le candidat produise un casier judiciaire vierge, il n'est pas nécessaire d'associer la Sûreté de l'Etat ou le SGRS au processus. L'autorité concernée peut alors prendre, elle-même, contact avec le fichier central judiciaire.

Le Comité permanent R plaide donc pour que l'on évite de recourir inutilement aux services de renseignement pour obtenir des informations disponibles à d'autres sources.

- ***Les données dont les services de renseignement disposent, sont-elles suffisamment précises pour servir de base à la prise d'une décision individuelle ?***

A l'occasion de l'examen de certains dossiers concrets, le Comité permanent R a déjà constaté des cas dans lesquels certaines données reprises dans des avis de la Sûreté de l'Etat étaient contestables, voire parfois erronées.

Si le rôle des services de renseignement n'est que de produire des analyses et des prévisions de tendances en matière de menaces pour la sécurité interne ou externe du pays, une erreur individuelle dans un dossier n'est pas nécessairement relevante. Il en est tout autrement si la personne sur qui porte l'erreur se voit refuser un droit, un avantage, une fonction ou une autorisation suite à des informations ou à un avis négatif d'un service de renseignement.

S'il s'avérait que les données recueillies par les services de renseignement dans le cadre de leurs missions légales (le suivi des menaces d'après des données collectées sur des groupes, sur des mouvements et des personnes) ne sont pas assez précises dans le cadre de vérifications de sécurité, il conviendra d'en tenir compte.

- ***La qualité des avis de la Sûreté de l'Etat est-elle suffisante ?***

Cette question se distingue de la deuxième en ce sens qu'il est possible de rendre un avis peu précis sur base d'un dossier pourtant bien documenté. En d'autres termes, que fait-on des fichiers et des renseignements d'un service de renseignement ? Peuvent-ils servir à une autorité administrative ?

Le Comité permanent R a déjà constaté des cas où des informations non recoupées provenant d'un « informateur » ont été transmises comme faits acquis à l'autorité de décision, comme s'il s'agissait de constatations effectuées directement par un membre des services de renseignement.

Dans ces cas, demandant des vérifications plus pertinentes, des erreurs administratives ne sont pas à exclure si ces vérifications ne sont pas effectuées.

2.4. Quel degré de transparence souhaite-t-on donner aux enquêtes, aux dossiers et/ou aux avis des services de renseignement ?

Le Comité permanent R pourrait-il exercer un « contrôle effectif et adéquat ? ». Comment le système mis en place pourrait-il offrir une réparation appropriée ?

La logique veut que les informations personnelles contenues dans les bases de données d'un service de renseignement puissent à certaines conditions, revêtir une certaine pertinence dans la prise de décision accordant, refusant ou retirant un droit, une qualité spéciale ou une agréation particulière à une personne déterminée.

Si l'on fait ce choix de confier, totalement ou partiellement selon les cas, l'exécution de certaines vérifications de sécurité à un service de renseignement, se pose alors la question du degré éventuel de classification qui s'applique au traitement des données, ainsi qu'au contenu et à la motivation de l'avis rendu.

Dans cette optique, un contrôle effectif et adéquat au sens de l'article 8 de la CEDH s'impose.

La nature de ce contrôle dépendra de l'option que l'on prendra entre la transparence totale et le secret le plus hermétique.

Le point de vue du Comité permanent R à ce sujet est de privilégier la plus grande transparence possible avec comme seule limite l'esprit et les dispositions de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité.

Le Comité permanent R estime en effet que l'on peut largement s'inspirer du système légal ainsi mis en place pour assurer, par similitude, une procédure de contrôle applicable à l'intervention des services de renseignement, dans le cas d'autres vérifications de sécurité que le législateur jugerait bon d'instituer.

Il s'agit là de la recherche d'un équilibre entre les deux solutions les plus extrêmes, à savoir :

- l'accès en tout temps par l'intéressé à l'ensemble de son dossier ;

- l'intéressé ignore totalement l'intervention d'un service de renseignement dans le traitement de son dossier ou n'a connaissance que d'un avis positif ou négatif émis par ce(s) service(s).

Dans la première éventualité, la personne concernée est à la fois celle qui est la mieux placée pour contrôler l'exactitude des données, mais du point de vue des services de renseignement, elle est aussi celle qui est la moins fiable pour y avoir accès et exiger des corrections éventuelles.

Cette solution n'apparaît donc pas compatible avec un fonctionnement efficace des services de renseignement dont les activités requièrent par nature l'application des dispositions légales en matière de classification et d'habilitations de sécurité.

Dans la seconde éventualité, le Comité permanent R pense par contre que le maintien du secret ne peut aller jusqu'à laisser une personne qui postule l'obtention d'un droit ou d'une autorisation spéciale, dans l'ignorance qu'un service de renseignement intervient dans la procédure pour délivrer un avis ou mener une enquête complémentaire.
Le Comité permanent R plaide donc pour que chaque vérification de sécurité soit soumise à l'accord préalable de la personne concernée et qu'à cette occasion, celle-ci soit mise au courant des démarches qui pourront être entreprises. Il faut aussi prévoir qu'en cas d'accord de la personne concernée, celle-ci puisse avoir connaissance de la motivation de l'avis, à l'exception des informations classifiées, et de l'existence d'un recours.

RECOMMANDATIONS GENERALES

Il faudrait que toute vérification des conditions de sécurité d'une personne opérée par un service de renseignement :

- soit fondée légalement ;

- soit portée préalablement à la connaissance de la personne concernée et que celle-ci y consente;

- donne lieu à des conclusions motivées, vérifiées et susceptibles d'être portées à la connaissance de la personne concernée ;

- soit assortie d'un droit de recours effectif qui permette à la personne concernée, sous réserve d'éventuelles données classifiées, de prendre connaissance de l'avis rendu à son sujet, de le contester et de présenter ses arguments.

La décision du service de renseignement devrait mentionner l'avertissement qu'un contrôle est possible par l'introduction de ce recours.

L'organe de recours devrait pouvoir rendre une décision effective en la matière.

Dans un premier temps, il suffirait déjà d'insérer les dispositions suivantes à la suite de l'article 34 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements :

« Dans le cas des recours introduits par des particuliers à la suite de l'avis rendu par un service de renseignement dans le cadre d'une vérification de sécurité, le Comité permanent R rend une décision motivée. Celle-ci est communiquée au requérant en tenant compte des éléments de sécurité pris en compte par les dispositions légales relatives à la classification et aux habilitations de sécurité ».

TITRE III : COMPOSITION ET FONCTIONNEMENT DU COMITE PERMANENT R

COMPOSITION ET FONCTIONNEMENT DU COMITE PERMANENT R

1. COMPOSITION

.Au cours de l'exercice écoulé, la composition du Comité dans toute ses parties a connu peu de changement.

Le Comité permanent R même comprend toujours, depuis le 19 septembre 2001, les membres suivants :

- monsieur Jean-Claude Delepière, Président,
- monsieur Gérald Vande Walle, Conseiller,
- monsieur Walter De Smedt, Conseiller

Nommés le 19 septembre 2001, pour un terme renouvelable de cinq ans[201], le terme de leur mandat se situe en septembre 2006.

Les président et membres suppléants restent également inchangés. Il s'agit respectivement de Messieurs Jean-Louis Prignon (magistrat fédéral), Etienne Marique (Président de la Commission des jeux de hasard) et P. De Smet (Substitut du Procureur général près le parquet de la Cour d'appel de Gand).

Depuis sa création, le Comité permanent R est assisté par son greffier, Monsieur Wouter De Ridder.

Le Service d'enquêtes R n'a pas connu, non plus, de grand changement et se compose toujours des cinq mêmes membres, le Chef du service compris.
Le Service d'enquêtes se trouve sous la direction de Monsieur Paul vander Straeten, Susbstitut du procureur général près la Cour d'appel de Mons, en congé.
Les membres sont détachés de la Sûreté de l'Etat, de la police fédérale et du SGRS.

L'administration du Comité permanent R comprend actuellement :

- un juriste
- une documentaliste,
- un comptable,
- deux secrétaires,
- une employée,
- un huissier,
- une réceptionniste,
- deux chauffeurs/collaborateurs logistique.

[201] Article 30 de la loi du 18 juillet 1991 organique du controle des services de police et de renseignement

2. ACTIVITÉS

Le lecteur trouvera, ailleurs dans ce rapport, un résumé des enquêtes de contrôle les plus importantes et une évaluation de l'activité du Comité permanent R en qualité d'organe de recours en matière d'habilitations de sécurité.

Comme institution indépendante du pouvoir exécutif, le Comité permanent R doit, et mieux encore, peut gérer lui-même son personnel, ses dépenses, etc … .
Cela implique qu'il doit lui-même organiser cette gestion des moyens humains et financiers.
Cela signifie également que les membres, le greffier et le personnel consacrent une part non négligeable de leurs activités au fonctionnement interne.

Bien que l'exercice des enquêtes de contrôle prennent parfois le pas sur le traitement des tâches administratives, cet aspect du fonctionnement interne du Comité permanent R ne peut être négligé car cette institution est soumise, comme l'ensemble des services publics fédéraux aux règles et procédures du droit public et administratif.

Lors du contrôle des services de renseignement, il peut ainsi être mieux à même de tenir compte d'une expérience propre des législations et des pratiques contraignantes, qui se situent entre le souhait et la réalité.

De surcroît, le Comité permanent R doit aussi assumer dans la pratique les conséquences de sa délicate mission. Il faut se référer, à ce sujet, à l'initiative prise en 2003 par le Comité permanent R d'organiser un colloque sur le renseignement en Belgique. Cette initiative a été reportée vu la sensibilité de ce secteur. Le Comité permanent R reprendra cette initiative ultérieurement parce qu'il estime qu'un débat public sur les services dits « secrets » est plus que jamais indispensable.

3. LES MOYENS FINANCIERS

Pour l'année 2002, la Chambre des représentants a approuvé une dotation de 1.997.780 euros. Cet exercice a été clôturé avec un boni de 278.984,49 euros.

Pour l'année 2003, une dotation de 2.014.000 euros a été approuvée. Les comptes de l'exercice budgétaire 2003 seront, comme à l'accoutumée après un contrôle interne et un contrôle de la Cour des comptes, présentés au Parlement.

Pour l'année 2004, un budget de 2.480.865 euros a été introduit et approuvé.

4. PARTICIPATION DU COMITE PERMANENT R A DES COLLOQUES, CONFERENCE ET AUTRES REUNIONS DE TRAVAIL

Au cours de l'année 2003, les membres du Comité permanent R ou de son Service d'enquêtes et de son personnel administratif ont participé aux réunions de travail, séminaires, conférences et colloques suivants :

- 21 mars 2003 : Faculteit der Rechtsgeleerdheid van de V.U.B. – Brussel
  « *Strafrecht van nu en straks* »

- 4 avril 2003 : Commission nationale de contrôle des interceptions de sécurité – France (Paris)

- 7 avril 2003 : Chambre de Commerce et d'Industrie du Hainaut
  « *L'entreprise à l'affût du changement* »
  « Détectez les menaces et saisissez les opportunités grâce à la mise en place d'une cellule de veille »

- 9 avril 2003 : Institut Royal supérieur de défense – Bruxelles
  « *L'improbable équilibre géopolitique du désordre mondial* » - Guy Spitaels – Ministre d'Etat

- 5 mai 2003 : SCIP – France (Paris)
  Débat avec Bernard Carayon – Député du Tarn, chargé par le Premier ministre d'un
  « Rapport sur l'Intelligence Economique en France »

- 6 mai 2003 : Bibliothèque Royale de Belgique – Bruxelles
  « *Information : un coût, une valeur !* »

- 6 mai 2003 : Tijd Academie – Brussel
  « *Competitive & Business Intelligence* »

- 6 juin 2003 : Asis Europe Benelux – Brasschaet
  « *The Terrorist Threat in Europe* »

- 19 juin 2003 : SCIP – France (Paris)
  « Les produits d'analyse et d'information issus de la veille et leur marketing»
  « Archivage et document électronique »

- 24 juin 2003 : SCIP – France (Paris)
  « *Intelligence économique et réseaux d'entreprises* »

- 12 septembre 2003 : Ceram Sophia Antipolis/IHESI – France
  « *troisième rencontres en Intelligence Economique et Management des Risques ».*

- 9 octobre 2003 : Intituut van Forensische Auditoren (IFA) – Gent
  « *Inbeslagneming en verbeurdverklaring in strafzaken : een stand van zaken*

- 14 octobre 2003 : Belgacom – Bruxelles
  "*Videoconferentie security"*

- 15 octobre 2003 : BEP – Entreprises – Dinant
  « Séminaire sur la veille stratégique »

- 21 octobre 2003 : La cellule ReHGIS - Chambre de Commerce et d'Industrie du Hainaut - Charleroi
  « *L'information stratégique au service du management »*

- 6-7 novembre 2003 : Université de Technologie de Belfort – France
  « *Images et usages du secret »*

- 13 novembre 2003 : Comité permanent de contrôle des services de police – Palais d'Egmont – Bruxelles
  « *10 ans après … La fonction de police sous la loupe du Comité permanent P »*

- 18 novembre 2003 : Direzione Nazionale Antimafia – Italie – Rome

- 19 novembre 2003 : Institut Royal Supérieur de Défense – Bruxelles
  « *De uitbreiding van de EU. Invloed op GBVB en EVDB »*

- 26 novembre 2003 : Ecole royale militaire – Bruxelles
  « *L'opération ARTEMIS »*

- 4-5 décembre 2003 : Security Intelligence Review Committee
  Ottawa – Canada
  "*Peacekeeping Intelligence : New players, extended boundaries".*

La participation à ces diverses activités permet au Comité permanent R de compléter son information. Celle-ci est reprise, dans la mesure de sa pertinence, dans les rapports d'enquête du Comité permanent R.

C'est le cas notamment cette année-ci en ce qui concerne le rapport sur « *La protection du potentiel scientifique ou économique du pays : le rôle des services de renseignement privés et public ».(Cfr p. 78 du présent rapport)*

Un compte-rendu de la conférence « *Peacekeeping Intelligence »* est repris ci-après.

5. COLLOQUE "PEACEKEEPING INTELLIGENCE: NEW PLAYERS, EXTENDED BOUNDARIES", CANADA (4 - 5 DECEMBRE 2003)

5.1. Introduction

Deux délégués du Comité permanent R ont pris part à la conférence du 4 et 5 décembre 2003 à Ottawa à propos du renseignement lors d'opérations de maintien de la paix.

Ce colloque était intitulé : « *Peacekeeping intelligence : new players, extended, boudaries* » et était organisé par le « *Canadien Center of Intelligence and Security Studies de l'Université de Carlton* », en collaboration avec le *« Royal Military College of Canada* ».

Vu l'importance de telles missions pour les forces armées belges dans ce cadre et le rôle crucial des services de renseignement lors de ces opérations, le Comité permanent R a décidé d'assister à ce colloque.

Ci-dessous sont mentionnées, sous forme résumée, quelques-unes des plus intéressantes thèses qui ont été présentées au cours de ce colloque. Ce résumé ne doit pas être considéré comme la retranscription littérale, mais bien comme une synthèse personnelle établie par la délégation du Comité permanent R, avec toute la réserve qui s'impose.

Les organisateurs du colloque publieront, dans le courant 2004, un livret reprenant les exposés qui ont été présentés.

Profitant de cette occasion, la délégation du Comité permanent R a également rendu visite à ses collègues canadiens du CSARS (Comité de surveillance des activités de renseignement de sécurité).

Il a été procédé à un échange de vues concernant la modification de la situation après le 11 septembre (à savoir la menace du terrorisme international et les réactions de la part des autorités, des services de renseignement et des services de contrôle). Le mode de contrôle, en particulier en ce qui concerne le traitement des plaintes introduites par des particuliers, a également été abordé.

5.2. Les constatations de base du colloque

La quasi-totalité des orateurs ont constaté l'émergence d'une nouvelle donne au sein de laquelle les missions de renseignement trouvent à présent leur place au cours d'opérations de maintien de la paix.

Cette situation se caractérise de la manière suivante :

– Les rapports de force sur le plan politique et militaire ont été radicalement modifiés depuis l'implosion du bloc soviétique. Cependant, toutes les structures de cette époque n'ont pas encore été adaptées aux nouvelles données.

- Le contexte international des services de renseignement est devenu particulièrement complexe en fonction d'éléments tels que la mondialisation, les révolutions technologiques, le foisonnement des informations, etc… tout comme les phénomènes tels que la désintégration d'Etats (essentiellement dans les régions peu développées), la radicalisation de grands groupes de populations, le terrorisme international et le crime organisé.

- Cette incertitude est encore renforcée par l'intervention accrue d'acteurs privés et d'ONG de natures très diverses dans tous les domaines, même dans l'armée.

Les Etats et l'ONU ont encore beaucoup trop fondé leurs opérations de maintien de la paix sur le modèle classique où il suffisait, de positionner quelques troupes militaires de pays neutres et de rallier les parties belligérantes aux accords de pacification du pays ou de la région, pour au moins permettre de conserver le statu-quo existant.
De telles opérations subsistent toujours (cfr. Chypre), mais sont devenues relativement exceptionnelles. Dans ces situations-là, il suffit d'une présence quasi-statique de troupes, par exemple à un poste frontière, ce qui n'exige qu'un besoin très limité de renseignements.

Ces opérations étaient toujours menées sur base du principe de la souveraineté des Etats et de la parfaite neutralité de l'ONU. Dans ce cadre, les commanditaires des opérations de maintien de la paix considéraient tout ce qui touchait au renseignement comme « louche » et « à ne pas faire ».

5.3. Les dures leçons

Cette conception classique des opérations a largement fait son temps.

La grande nouveauté tient à présent dans le fait que les opérations de maintien de la paix trouvent de plus en plus de place dans un environnement hostile où, tant le but même de l'opération, que la sécurité des troupes participantes soit mis en péril.

Les pays intervenants - et encore moins les organisations internationales - n'étaient pas préparés à faire face à ce nouveau contexte confus. C'est ce qui a entraîné de sévères débâcles dans diverses opérations de maintien de la paix, des opérations qui ont échoué, ou qui ont présenté d'importants manquements.

Plusieurs orateurs se sont penchés sur les causes de ces échecs.

De nombreuses explications, pas toujours concordantes d'ailleurs, sont données. Le mandat des troupes intervenantes, la marge de manœuvre opérationnelle du commandement sur place, les troupes elles-mêmes, et leur équipement, ont certainement beaucoup d'importance dans le déroulement des opérations. Mais d'après la plupart des orateurs, un facteur commun aux divers échecs subis doit être recherché dans l'absence ou dans la non utilisation du renseignement.

Ces échecs ont mené, tant pour l'Onu que pour les troupes et les pays participants, à la refonte du mode d'exécution des opérations de maintien de la paix. On s'est aperçu qu'une activité permanente de renseignement, même préalable à la mise en place de troupes, constituait une exigence absolue.

5.4. Renseignements : le tout n'est pas de les vouloir !

Par cette affirmation, on estime qu'une chose est de reconnaître l'intérêt concret du renseignement pour ces missions, mais qu'il en est une autre de réaliser cette condition sur le terrain.

Lors de la mise en œuvre concrète de l'activité de renseignement, on rencontre d'ailleurs de très nombreux problèmes.

1. Si l'on part du principe selon lequel un pays qui fournit des troupes pour des opérations de maintien de la paix, peut y inclure une mission pour ses services de renseignements divers problèmes se posent. La connaissance du pays ou de la région de l'opération n'est pas toujours évidente à acquérir. D'innombrables facteurs peuvent s'avérer d'un intérêt crucial. Les cibles classiques des services de renseignement tels que des opposants potentiels ou une milice en particulier ne sont plus les seuls aspects intéressants.

   Outre la quantité, l'armement, les intentions, la position, etc … des belligérants, il est aussi important de savoir quelle est l'opinion de la population locale, l'état des routes, les us et coutumes, le climat, les intérêts économiques spécifiques.

   De telles connaissances ne sont pas évidentes à acquérir et à actualiser. Un obstacle important pour y arriver est par exemple la connaissance de la langue (ou du dialecte) et de la culture de la région en question.

2. En deuxième lieu, les renseignements obtenus doivent être utiles au commanditaire de l'opération de maintien de la paix, à savoir l'ONU et le commandant local de la force de paix.

   Dans les deux cas, ces renseignements ne sont pas faciles à obtenir.

   En ce qui concerne le premier point, une évolution a eu lieu au sein de l'ONU. Auparavant, cette organisation considérait la collecte de renseignements et d'informations comme une immixtion dans les affaires intérieures d'autres pays, pouvant même à certains endroits être punissable.

   Rien que sur le plan juridique, il s'agit là en effet d'une question épineuse, si l'on se base sur les principes classiques du droit international public.

   L'attitude actuelle est toutefois devenue bien plus pragmatique, suite aux leçons tirées du passé. Ainsi l'ONU, ne nie plus à présent, la nécessité du renseignement et le juge même indispensable pour la bonne exécution des opérations de maintien de la paix.

   Au sein même du Secrétariat Général et du Conseil de Sécurité des Nations Unies, on constate une impulsion vers une intégration organique du renseignement. Cette nouvelle politique va de pair avec une meilleure harmonisation du mandat des troupes engagées et un cadre plus clair pour le commandement local.

3. Considérant qu'un pays déterminé participant à d'une force d'intervention commune avec d'autres partenaires, parvient à produire des renseignements, la question se pose de savoir si ceux-ci seront transmis au commandement local et seront également partagés avec les autres pays.

   Cette question peut paraître surprenante pour les observateurs extérieurs, mais elle constitue le signe évident que chaque pays partage avec prudence les renseignements qu'il obtient.

   On ignore à ce sujet les objections classiques telles que la protection des sources, la protection des capacités techniques de renseignement du pays (par exemple : les satellites ou les interceptions de communications), la protection des canaux d'échanges bilatéraux ou multilatéraux .

   Par ailleurs, quasiment chaque pays a sa propre conception du renseignement et du mode selon lequel il s'acquiert. Il existe à ce sujet une importante distinction en fonction de l'utilisation ou non dans le renseignement de « covert actions », (à savoir des opération offensives, voire clandestines).

   Dans le contexte spécifique des opérations de maintien de la paix, il convient cependant de tenir compte d'autres facteurs essentiels. Une grande différence est faite par ceux qui composent la coalition intervenante et par ceux qui en ont la charge. Il est clair et évident que, par exemple, la collaboration pour le maintien de la paix se passe mieux entre troupes appartenant à des pays membres de l'OTAN, même si à ce niveau, les intérêts nationaux peuvent parfois diverger. Sans le dire clairement, il n'est donc pas exclu que certains participants témoignent également d'un « intérêt particulier » pour leurs partenaires dans la coalition. Il ressort cependant clairement de nombreux témoignages que lors des dernières opérations, l'échange de renseignements entre pays participants et le commandement de l'opération n'a été qu'un vœu bien trop peu souvent concrétisé. La confiance mutuelle entre les parties est donc très loin d'être une chose acquise.

   Cette situation n'est pas seulement liée à la composition des forces d'intervention mises en œuvres. Il faut également reconnaître que les renseignements récoltés peuvent aussi servir à d'autres fins que la réussite de l'opération elle-même, tels que les intérêts militaires, politiques, et même économiques propres aux Etats qui envoient leurs troupes ou qui, d'une manière ou d'une autre , sont impliqués dans le conflit.

   Il est actuellement impensable que des services ou unités de renseignements actifs dans une zone d'opérations ne fassent pas (avant tout) rapport à leurs propres quartiers généraux.

5.5. Evolutions

5.5.1. Un meilleur échange de renseignements

Les plus récentes opérations montrent une amélioration de la collaboration dans le domaine du « partage de l'information », même si celui-ci demeure difficile et non obligatoire.

Il faut à cet effet garder à l'esprit l'objectif premier, à savoir l'amélioration des conditions de vie dans les régions concernées et la poursuite de l'intérêt commun dans le cadre du droit international par une utilisation adaptée des moyens militaires ou autres.

Un orateur a proposé de modifier le concept du « besoin d'en connaître » (need to know) par celui du « besoin de partager » (need to share).
Selon certains orateurs, le monde du renseignement n'en reste pas moins soumis à une évaluation éthique.

5.5.2. L'intégration du renseignement dans l'ensemble des opérations de maintien de la paix.

La composante du renseignement n'est pas uniquement importante pour le soutien des activités opérationnelles et tactiques des militaires.

Elle est plus vaste à deux égards :

- d'une part, le renseignement dans les opérations de maintien de la paix est indispensable au niveau des décisions stratégiques, tant au niveau national qu'international, et n'est pas des moindres pour l'ONU.
- d'autre part, les opérations actuelles de maintien de la paix ne se limitent plus simplement à une mission purement militaire.

La mission de maintien de la paix est actuellement considérée comme la collaboration continue de la communauté internationale, qui va de la prévention des conflits pour aboutir à la reconstruction du pays ou de la région concernée.

Parmi ces tâches, on retrouve une vaste gamme d'activités, tant pour les organisations militaires que civiles (et même privées comme des ONG).
Presque chaque jour, on peut observer dans les médias des opérations de maintien de la paix qui comprennent toutes sortes de tâches diversifiées comme la protection des réfugiés, l'aide médicale, le maintien de l'ordre, la stabilisation, le désarmement, l'arrestation de criminels de guerre, etc. Le concept de maintien de la paix a tellement évolué en ampleur et en profondeur que certains trouvent que le terme même de maintien de la paix est quelque peu dépassé. Le renseignement doit donc pouvoir être utilisé pour des missions fort diversifiées.

5.5.3. Exigence supérieure de qualité pour le renseignement

Pour répondre à ces besoins croissants de renseignement, les services de renseignement se doivent de travailler mieux et plus rapidement.

Pour autant qu'ils l'aient eu un jour, ces services ont en outre perdu leur monopole de producteurs de renseignements. A titre d'exemple, une ONG peut rédiger des rapports fiables quant à la présence d'armes légères dans une région déterminée. Ceci est notamment possible grâce à des collaborateurs de terrain qui réalisent des interviews sur place.

Les services de renseignement, essentiellement militaires, disposent cependant de possibilités qui n'existaient pas, ou à peine, auparavant, surtout dans le domaine des sources non humaines. Plusieurs orateurs plaident par conséquent pour le recours, dans une proportion adéquate à des sources humaines et non humaines, y compris les sources ouvertes, dont l'intérêt va croissant.
Celles-ci ne viennent pas remplacer les sources les plus classiques, comme les informateurs, mais elles peuvent confirmer et compléter les informations ainsi obtenues ou mieux centrer l'intervention de l' « humint » (intelligence humaine).

Par ailleurs, les sources ouvertes utilisées de manière professionnelle, semblent pouvoir contribuer à un produit fini de très haute qualité.

La technologie moderne peut également contribuer à offrir une grande quantité d'informations de manière structurée aux commandements et aux responsables politiques. Il n'est d'ailleurs pas suffisant de produire des renseignements corrects, il faut également les intégrer dans les prises de décisions. Ceci suppose, non seulement, une présentation utilisable d'une masse de données, mais également une aptitude des décideurs à savoir gérer le renseignement.

L'utilisation des ressources de la technologie moderne ne s'oppose qu'en apparence, à la conception qui veut que les services de renseignement dépendent, aussi peu que possible sur le terrain, de ces moyens technologiques.
C'est seulement la pratique qui montre si les outils techniques ingénieux sont suffisants par rapport aux exigences du terrain en question.

5.6. Une préparation correcte

Une des conditions souvent rappelée par les experts de terrain, et partagée par les chercheurs, est que les troupes et commandements déployés doivent être correctement préparés afin de réagir de manière adéquate aux éventuelles complications. Ceci implique entre autres, comme déjà indiqué ci-dessus, qu'il convient autant que possible de procéder à l'échange d'informations avec d'autres services.

Il est important d'éviter de laisser se creuser un gouffre – ce qui est apparemment typique dans de telles opérations – entre d'une part le commandement et les troupes sur place, et d'autre part, les quartiers généraux des services de renseignements nationaux et l'ONU. Afin d'éviter un tel écart, il faut en permanence veiller au contact et à la transparence.

Enfin, il est vital que tant les troupes présentes sur le terrain que les quartiers généraux aient une bonne perception de la situation réelle dans la région, ce qui implique entre autre que les unités et certainement les cellules de renseignement sur place ne considèrent pas uniquement la problématique d'un point de vue occidental. Pour obtenir une idée correcte de la situation, il faut une « prise de conscience permanente» qui tienne également compte des spécificités et mentalités de la population locale

ENVOI AUX MINISTRES DE LA JUSTICE ET DE LA DÉFENSE NATIONALE

Le 20 avril 2004, le présent rapport a été transmis, pour avis, à Madame L. ONKELINX, Vice-Première ministre et ministre de la Justice et à Monsieur A. Flahaut, ministre de la Défense nationale.

Madame ONKELINX n'a fait parvenir aucun commentaire au Comité permanent R.

Par courrier du 1er juin 2004, Monsieur le ministre de la Défense nationale a adressé la lettre suivante au Comité permanent R :

« *Le rapport général d'activités 2003 de votre Comité permanent de contrôle a retenu toute mon attention.*

J'ai particulièrement lu avec beaucoup d'intérêt votre étude concernant la protection du potentiel scientifique et économique et le rôle des services de renseignements privés et publics dans cette matière, étude dont je partage pleinement vos conclusions et recommandations. La problématique mérite à mon avis une discussion approfondie au Comité ministériel du Renseignement et de la sécurité.

En ce qui concerne les rapports d'enquêtes dans lesquels le SGRS est cité, j'ai déjà eu l'occasion de formuler mon avis lorsque vous m'avez présenté les rapports individuels relatifs à chaque enquête.

En tenant compte de ce qui précède, je ne vois pas d'inconvénient à ce que le projet de rapport général, tel que vous me l'avez fait parvenir, soit rendu public ».

APPROBATION PAR LES COMMISSIONS PARLEMENTAIRES

Le 18 juin 2004, les commissions de suivi du Sénat et de la Chambre des représentants ont approuvé, à l'unanimité, le rapport d'activités 2003 du Comité permanent R.